2006-12

Policing toward a de-clawed jihad antiterrorism intelligence techniques for law enforcement

Gyves, Clifford M.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

POLICING TOWARD A DE-CLAWED JIHAD: ANTITERRORISM INTELLIGENCE TECHNIQUES FOR LAW ENFORCEMENT

by

Clifford M. Gyves

December 2006

Thesis Co-Advisors: Thomas Bruneau
María Rasmussen

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2006	Master's Thesis, September 2005-December 2006

4. TITLE AND SUBTITLE Policing Toward a De-Clawed Jihad: Antiterrorism Intelligence Techniques for Law Enforcement

5. FUNDING NUMBERS

6. AUTHOR(S) Clifford M. Gyves

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Headquarters, Air Force Office of Special Investigations
Andrews AFB, MD 20762-7002

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

This thesis examines intelligence strategies that law enforcement officials may use to combat transnational Islamic terrorism in the United States. Many of the concepts discussed in this thesis come from U.S. Intelligence Community approaches. Others are familiar to both intelligence and law enforcement professionals. The thesis focuses on Islamic terrorism, most notably promoted and conducted by al-Qa'eda, though a number of the techniques can apply to other terrorist threats. The religious foundations of Islamic terrorism and the milieu in which it flourishes provides both a strategic and tactical backdrop for what has been cast as a global jihad—a violent, worldwide religious campaign with political objectives. The unique ethnic and religious characteristics also present specific challenges for law enforcement intelligence operations, most notably in collecting human intelligence. Processing collected threat intelligence and developing defensive plans require a broad, multi-layered strategy to be successful in meeting the challenges posed by a geographically pervasive terrorist threat. As this thesis argues, local jurisdictions must work in tandem with national-level organs to create an effective system that will identify and prevent potential terrorist operations in the United States.

14. SUBJECT TERMS Terrorism, Antiterrorism, Counterterrorism, Anti-Terrorism, Counter-Terrorism, Law Enforcement, Police, Intelligence, Human Intelligence, HUMINT, Source, Intelligence Analysis, Risk Assessment, Islamism, Islamist Terrorism, Islamic Fundamentalism, Transnational Terrorism, Salafism, Salafi, Salafist, Jihad, Global Jihad, Global Salafi Jihad, Terrorist Network, Network

15. NUMBER OF PAGES
179

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

POLICING TOWARD A DE-CLAWED JIHAD: ANTITERRORISM INTELLIGENCE TECHNIQUES FOR LAW ENFORCEMENT

Clifford M. Gyves
Major, United States Air Force
B.S., United States Air Force Academy, 1991
M.A., The University of Arizona, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Clifford M. Gyves

Approved by: Dr. Thomas Bruneau, PhD
Thesis Co-Advisor

Dr. María Rasmussen, PhD
Thesis Co-Advisor

Dr. Douglas Porch, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis examines intelligence strategies that law enforcement officials may use to combat transnational Islamic terrorism in the United States. Many of the concepts discussed in this thesis come from U.S. Intelligence Community approaches. Others are familiar to both intelligence and law enforcement professionals. The thesis focuses on Islamic terrorism, most notably promoted and conducted by al-Qa'eda, though a number of the techniques can apply to other terrorist threats. The religious foundations of Islamic terrorism and the milieu in which it flourishes provides both a strategic and tactical backdrop for what has been cast as a global jihad—a violent, worldwide religious campaign with political objectives. The unique ethnic and religious characteristics also present specific challenges for law enforcement intelligence operations, most notably in collecting human intelligence. Processing collected threat intelligence and developing defensive plans require a broad, multi-layered strategy to be successful in meeting the challenges posed by a geographically pervasive terrorist threat. As this thesis argues, local jurisdictions must work in tandem with national-level organs to create an effective system that will identify and prevent potential terrorist operations in the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PURPOSE....1
B. CONTEXT....1
C. BACKGROUND ON ISLAMIST TERRORIST METHODOLOGY....2
D. HUMAN INTELLIGENCE AND ANALYSIS....3
E. LAW ENFORCEMENT ANTITERRORISM METHODS AND MEASURES....4
F. THESIS SYNOPSIS....5
G. A NOTE ON SPELLING, RENDITION OF FOREIGN TERMS, AND DATE CONVENTIONS....6

II. ISLAMIST TERRORIST METHODOLOGY....7
A. STRATEGY AND VISION....8
1. The Strategic Plan....8
2. Terrorist Warfare Evolving....10
3. Information Operations....11
B. TOOLS, TACTICS AND TECHNIQUES....13
1. Innovators or Imitators?....14
2. Intelligence....18
3. Mass Casualty Attacks....20
C. LESSONS FOR ANTITERRORISM OFFICIALS....24

III. THE JOY OF HUMAN INTELLIGENCE: ITS UNIQUE APPLICATION TO HOMELAND SECURITY AND ANTITERRORISM....27
A. EMERGING ROLES IN PREVENTIVE POLICING THROUGH INTELLIGENCE COLLECTION AND EXPLOITATION....27
B. HUMINT IN LAW ENFORCEMENT....30
C. LOOKING FOR CLUES—JUST WHAT ARE WE LOOKING FOR?....32
1. Indicators of Terrorist Presence....33
2. Individual Terrorist Network Members....33
3. Indicators of Terrorist Activity....35
D. TYPES OF HUMINT AVAILABLE TO LAW ENFORCEMENT – THREE LAYERS....38
1. Public Awareness Campaign....38
2. Open Contacts....40
3. Confidential Informants....40
E. SOURCE ACCESS....41
1. Unassociated Observers....41
2. Proximal Outsiders....41
3. Detached Associates....42
4. Network Members....42
F. SOURCE PLACEMENT....42
G. SOURCING IN AN ETHNIC IMMIGRANT COMMUNITY....44

1. Reducing Fear, Building Trust 44
2. Using the Stick 46
3. Using the Carrot 46
4. Finding the Focal Point 47

IV. ANTITERRORISM ANALYSIS FOR THE LAW ENFORCEMENT COMMUNITY: PUTTING THE PIECES TOGETHER 49
A. A LOST ART 50
B. INTELLIGENCE FAILURES: EYE ON ANALYSIS 50
C. BROAD GOALS OF TERRORISM ANALYSIS 52
D. ILLUSTRATING THE PRESENT 53
E. PREDICTING THE FUTURE 54
F. TERRORIST ATTACK PROCESS INDICATOR SEQUENCE 56
G. THE ANALYSIS PROCESS 59
H. THE SCIENCE OF ANALYSIS 61
I. THE VOLUME CHALLENGE 69
J. AUTOMATED ANALYTICS AND DATA MINING 71
K. STRUCTURING LAW ENFORCEMENT INTELLIGENCE ANALYSIS FOR ANTITERRORISM 74
L. HARNESSING ANALYSIS FOR THE FUTURE 76

V. COVERING ASSETS: INTELLIGENTLY FOCUSED DEFENSIVE ACTIONS 79
A. THREAT-BASED ASSESSMENTS AND PLANNING 80
1. Threats, Vulnerabilities and Countermeasures 82
2. Ulterior Motives 84
3. Collateral Consequences 84
4. At What Cost? 88
B. PLANNING FOR SECURITY: A PROPOSED METHODOLOGY 90
1. Prioritizing Potential Targets 90
2. Severity Matrix 92
3. Probability Matrix 94
4. Cross-Feeding the Matrices 97
C. CONCLUSION 98

VI. CONCLUSION 99

APPENDIX A. AL-QA'EDA INTELLIGENCE REQUIREMENTS 103
A. FOR TARGETING AN INDIVIDUAL PERSON 103
B. FOR TARGETING A FACILITY OR ACTIVITY 103

APPENDIX B. EXAMPLE SOURCE OPERATIONS 105

APPENDIX C. AUTOMATIC ANALYTICS: FROM FIELD REPORT TO DATABASE 121

APPENDIX D. MULTI-MATRIX METHOD: EXAMPLE ASSESSMENT 123

LIST OF REFERENCES 129

BIBLIOGRAPHY 141
INITIAL DISTRIBUTION LIST 159

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1 Law Enforcement Intelligence Roles....30
Figure 2 Indicator Chain....57
Figure 3 Indicator Chain – Reconnaissance....57
Figure 4 Indicator Chain – Time Check....58
Figure 5 Indicator Chain – Staging....58
Figure 6 Indicator Chain – Forecast....59
Figure 7 The Intelligence Cycle....60
Figure 8 Isolating a Key Node....65
Figure 9 Newly Activated, Previously Unknown Node....66
Figure 10 Newly Activated, Redundant Link....66
Figure 11 Layered Analytical Network Structure....75
Figure 12 Regional Analytical Cooperation....76
Figure 13 Risk Assessment Matrix....92
Figure 14 Severity Sub-Matrices....93
Figure 15 Severity Matrix (HLS-CAM)....94
Figure 16 Probability Matrix....95
Figure 17 Probability Sub-Matrices....96
Figure 18 Risk Assessment Process....97
Figure 19 Example Damage Estimates for Each Asset....125
Figure 20 Example Severity Matrix Calculation....126
Figure 21 Example Vulnerability Sub-Matrix Estimates for Each Asset....127
Figure 22 Example Probability Matrix Calculation....127
Figure 23 Example Risk Assessment Matrix Calculation....128

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY

agent 1. *n.*, (in context of police roles) law enforcement officer in plain clothes, such as a federal agent or detective
2. *n.*, (Intelligence Community term) a recruited human source of Information

analyst *n.*, one who analyzes raw intelligence to put it in context and derive meaning from it; produces *finished intelligence*. (Also used in context of police roles.)

analytics *n.*, computerized analytical algorithms

asabiya (Arabic) *n.*, tribal or group loyalty

asset *n.*, (intelligence term) a recruited source of information; synonymous with *agent*

Caliphate (derived from Arabic) *n.*, the unified Islamic Nation, governed by one leader (the Caliph) who commands political and religious authority with God's (Allah's) blessing

confidential informant (police term) *n.*, one who provides information to police and whose identity is protected

data mining *n.*, cross-referencing data elements to discern patterns, links and associations among them

detached associate *n.*, person from whom terrorist(s) depend on for some measure of routine service or support (grocer, cleric, landlord, etc.), but who may not necessarily endorse the terrorist agenda

finished intelligence *n.*, intelligence that has been analyzed and interpreted

halal (Arabic) *n.*, Islamic dietary strictures; *adj*., of or relating to halal

HUMINT *n.*, acronym for *human intelligence*, or intelligence derived from human sources of information

imam (Arabic) *n.*, local Muslim cleric

indicator *n.*, (intelligence term) something observable that will likely occur as a stage in a developing incident or scenario

indication	*n*., (intelligence term) occurrence that has already happened that fits into an *indicator* category
Islamism	(derived from Arabic) *n*., a political ideology in which Islam should be universally applied to all facets of society, from personal religious practices to government and politics
Islamist	(derived from Arabic) *adj*., of or relating to Islamism; n., one who ascribes to an Islamist ideology
jihad	(Arabic) *n*., religious struggle; sometimes used for "holy war"
jihadi	(Arabic) *adj*., of or relating to jihad; *n*., one who endorses or engages in violent jihad; generally used in reference to radical activists[1]
jihadist	(derived from Arabic) *adj*., relating jihad as a political ideology; *n*., one who ascribes to jihad as a political ideology
mujahed	(Arabic) *n*., holy warrior, singular (similar to *jihadi*, but used to denote a soldier in war)
mujahedin	(Arabic) *n*., plural of *mujahed*
mukhtar	(Arabic) *n*., "the elected one," elder who serves as the de facto leader of a traditional Arab community
modus operandi	(Latin) *n*., method of operations. Also known by its acronym *MO*.
network link	*n*., a connection or relation between two given network *nodes*
network member	*n*., a witting, bona fide member of a terrorist network
network node	*n*., an individual or entity (such as a terrorist cell) in a network
open contact	*n*., one who provides information to police openly without the need for confidentiality
patrolman	(in context of police roles) *n*., uniformed patrol officer

[1] Fawaz A. Gerges, *The Far Enemy: Why Jihad Went Global* (New York, NY: Cambridge University Press, 2005), p. 330.

proximal outsider — *n.*, person tangentially affiliated with suspected terrorists, or who is in close proximity to them

salaf — *n.*, the Prophet Muhammad and his first generation of disciples

Salafi — (Arabic) *adj.*, of or relating to form of Islamic fundamentalists practice predicated on an adherence to a lifestyle emulating that if the *salaf*; n., one who professes to Salafi form of Islam

Salafism — (derived from Arabic) *n.*, a religious and political ideology founded on Salafi Islam

Salafist — (derived from Arabic) *adj.*, of or relating to the ideology of Salfism; *n.*, one who follows Salafist ideology

sharia — (Arabic) *n.*, Islamic law

source — 1. *n.*, a source of information
2. (law enforcement term) *v.*, to recruit or employ someone as a source; to manage a collection operation using sources, commonly called *sourcing*

source access — *n.*, describes the kind of information a source can routinely obtain on terrorists or terrorist activity

source placement — *n.*, situation or physical location that affords a source access to information about terrorists or terrorist activity

surveil — *v.*, (police and intelligence term) to conduct surveillance

surveillant — *n.*, (police and intelligence term) one who conducts surveillance; member of a surveillance team

umma — (Arabic) *n.*, the "community of the faithful," the global Muslim community

unassociated observer — *n.*, person who lives or works in a location from which he may observe pre-operational terrorist preparation, such as target surveillance or supply acquisition, but is not expected to have direct contact with terrorists

zakat (Arabic) *n.*, Islamic charitable contributions (similar in principle to Christian tithing, but traditionally mandated at 2.5 percent of one's income)

ACKNOWLEDGMENTS

I would like to thank, first and foremost, my wife Suzanne, and my children, Grant and Paxton, for their patience. I played the hermit during this long process, sequestered for hours upon days composing this thesis to the neglect of my family. Now it's time to get reacquainted.

Many friends, colleagues and mentors guided me on this journey. I would like to thank my thesis advisors, Professors María Rasmussen and Tom Bruneau, for combing through innumerable pages of drafts, and for keeping me on track. I would also like to thank Professor Craig Hooper for his time, insight and encouragement. Professor Brian Swanland gets the credit (or the blame) for directing me on this thesis path, and his support has been tremendous. Jacob Shapiro of Stanford University piqued my interest in exploring and questioning organizational dynamics within the global terrorist network, and his own research and mentorship in the area served as a great springboard for my own. Professor Tom Johnson's encouragement and technical materials on directed graph theory, and Tara Leweling's resource leads, deepened my understanding of social network theory and enabled me to make a critical examination of the global terrorist apparatus.

Nancy Sharrock, my thesis editor, worked magic on the drafts to bring the product up to standard. Sam K., Steve Rocke, Bill Boitnott, Rory Sutton, Sargon Yalda and Joe Odisho answered my questions, shared their first-hand knowledge and helped me give this thesis some real-world perspective. And whenever I'd feel the crunch, I'd reflect on Chuck Daenzer's faith in my ability to tackle this project, and how patiently he's been waiting for the manuscript.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

This thesis examines possible government options in response to Islamist transnational terrorist activity in the United States. The objective is to illuminate what intelligence techniques domestic law enforcement officials may employ to increase their effectiveness.

The overall question that this thesis seeks to answer is: What intelligence techniques should domestic law enforcement officials apply to thwart Islamist transnational terrorism? A subset of questions, from general to specific, includes:

- What indicators do terrorist activities present?
- How might law enforcement officials best observe those indicators?
- What techniques do intelligence organizations employ that law enforcement may use or modify to suit their own operations?

B. CONTEXT

How can law enforcement officials use intelligence to curb or prevent Islamist terrorist activity in the United States? A handful of authors have put forward "street-level" techniques, such as the use of informants and open contacts[2] or the employment of pre-operational attack indicators,[3] though not in a comprehensive format related to law enforcement intelligence. These few publications notwithstanding, most proposed intelligence-related solutions tend to aim at national policy or the strategic level, with little concrete, tactical advice for law enforcement professionals. Writings on intelligence related to terrorism fail to consider the law enforcement dimension in significant depth.[4] A study of general concepts in intelligence, however, can enhance the

[2] Cliff Mariani, *Terrorism Prevention and Response: The Definitive Law Enforcement Guide to Prepare for Terrorist Activity*, 2nd Edition (New York, NY: Looseleaf Law Publications, Inc., 2004), pp. 126-133; *A Law Enforcement Guide to Understanding Islamist Terrorism* (Baton Rouge, LA: First Capital Technologies, LLC., 2003), pp. 67-80.

[3] Ibid., pp. 19-21, 100-104, 110-111.

formulation of both strategic and tactical intelligence applications for police antiterrorism programs, particularly in the areas of collection strategies, analysis processes and asset protection measures. The geographically pervasive threat of Islamist terrorism necessitates a layered, multi-echelon response, such that the intelligence tools presented in the thesis should be integrated into a cohesive, national effort. This is especially true in the realm of intelligence analysis and risk assessment, where independent, uncoordinated efforts by multiple local jurisdictions will fall short of meeting the threat.

C. BACKGROUND ON ISLAMIST TERRORIST METHODOLOGY

The thesis addresses specific strategies and methodologies of the Islamist terrorist threat, in order to delimit the scholarly focus to this subset of transnational terrorism. Al-Qa'eda has assumed the mantle of a global Islamist jihad, acting as the vanguard of a protracted campaign against the West. It promulgates a strategic vision, as well as tactical direction and education, to its geographically distributed affiliates, greatly aided by the Internet. By sharing a common vision and exchanging tactical practices, the dispersed terrorist cells collaborate in a way that guides them toward common methodological principles. These commonalities become evident in case studies of past terrorist attack operations, case studies from which both the terrorists themselves and antiterrorist officials draw lessons. Numerous authors present case studies and analyses of transnational terrorist methodologies. One striking theme that emerges is that terrorists use tactics that have been attempted or proven effective in the past.[5] This tendency for terrorists to follow tactical precedents might offer authorities a weakness they can exploit through focused intelligence collection and analysis, most often derived from human sources.

---

[4] For examples, see Philip B. Heymann, *Terrorism, Freedom, and Security: Winning without War* (Cambridge, Massachusetts: The MIT Press, 2003); Brian Michael Jenkins, *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy* (Santa Monica, CA: RAND, 2002); Paul K. Davis and Brian Michael Jenkins, *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, CA: RAND National Defense Research Institute, 2002); *Defeating the Jihadists: A Blueprint for Action*, *Century Foundation Task Force*, Richard A. Clarke, chairman (New York, NY: The Century Foundation Press, 2004); Stephen Sloan, *Beating International Terrorism: An Action Strategy for Preemption and Punishment*, revised edition (Maxwell AFB, AL: Air University Press, 2002); Paul Pillar, *Terrorism and U.S. Foreign Policy*, paperback edition (Washington, DC: Brookings Institution Press, 2003).

[5] Jason Burke, *Al-Qaeda: The True Story of Radical Islam* (New York, NY: I.B. Tauris & Co. Ltd., 2004), p. 236; Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York, NY: Copernicus Books, 2003), p. 236; Pillar, "Fighting International Terrorism," p. 19.

D. HUMAN INTELLIGENCE AND ANALYSIS

One theme permeates the literature on intelligence: more (or better) human intelligence (HUMINT) is required to fight terrorism effectively. This appears to be the consensus, from the 9/11 Commission to *op ed* pieces.[6] American reliance on technical intelligence collection platforms (like signals or imagery intelligence) left the intelligence community ill-informed on the growing threat and attack plans by al-Qa'eda. One common thread attributes part of the 9/11 "intelligence failure" to an inability to analyze raw information and develop a predictive outlook on al-Qa'eda's impending operations. Sundri Khalsa asserts that collection was not a factor in the failure, though the intelligence community and its stakeholders historically tend to react to such failures with a misplaced emphasis on collection; rather, she characterizes the 9/11 debacle as an analytical failure.[7] Thomas Dowling and Paul Pillar suggest analysts failed to interpret the available information accurately.[8]

Colleen McCue, like Khalsa, recognizes the tendency to fix intelligence problems by focusing on information collection and sharing, but stresses the need to bolster analytical capabilities.[9] Often, there is too much information for human beings to analyze, which Jonathan White argues contributed to the 9/11 failure.[10] McCue and

---

[6] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, authorized Edition [paperback] (New York, NY: W.W. Norton & Company, Inc., [2004]), pp. 415; Ralph Peters, "The Case for Human Intelligence," *Armed Forces Journal* (July 2005): 24-26; Mark V. Kauppi, "Counterterrorism Analysis 101," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 43; Robert L. Hubbard, "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 71.

[7] Captain Sundri K. Khalsa, USAF, "Terrorism Forecasting: A Web-Based Methodology," *Occasional Paper Number Eleven* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004), pp. 1-2, 21. While this author's own experience as a collector exemplifies Khalsa's perspective regarding the post-incident emphasis on collection, others point to different reactions within the Intelligence Community. Michael Handel illustrates reactions within the analytical community that do not necessarily call for more information. Rather, the analysts focus on methodological reforms (to overcome biases); organizational reforms (to improve objectivity or reduce negative political influences), or "precautionary measures" (whereby the analysts hedge their bets and offer "worst case" analysis. (See Michael I. Handel, "Intelligence and the Problem of Strategic Surprise," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, eds. Richard K. Betts and Thomas G. Mahnken [Portland, OR: Frank Cass Publishers, 2003], pp. 19-22.)

[8] Thomas Dowling, "Failures of Imagination: Thoughts on the 9/11 Commission Report," *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 13-15; Pillar, "Fighting International Terrorism," p. 20.

[9] Colleen McCue, "Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism," *Defense Intelligence Journal*, vol. 13, nos. 1 & 2 (2005): 47.

[10] Jonathan R. White, *Defending the Homeland: Domestic Intelligence, Law Enforcement and Security* (Canada: Wadsworth/Thomson, 2004), pp. 23-25.

Khalsa advocate using automated analytical tools to handle the massive quantities of data, since they can process the information more effectively, efficiently and objectively than human analysts alone.[11] Nevertheless, the human analyst must interpret the results that the automated system generates, in order to ascribe meaning to them in the proper context.

Analysts face the daunting task of characterizing the terrorist threat and predicting future terrorist operations, and they must remain cognizant of common mental biases that may mislead them. One recent school of thought suggests the Islamist threat has devolved into a loose, global network that is overwhelmingly decentralized. Scholars and analysts must take special care to avoid some pitfalls such a view may present. Notably, general characterizations of the global network can oversimplify it, painting it as completely decentralized and virtually leaderless. Such generalizations ignore the heterogeneous nature of the global apparatus and overlook elements of the network where hierarchical structure and centralization persist. Furthermore, the appeal of network concepts may induce planners to adopt decentralized, network-centric approaches to fighting terrorism at the expense of proven, centralized operations.

A general examination of human intelligence and attendant analysis thereof provides a promising context for intelligence in law enforcement antiterrorism efforts, since the bulk of law enforcement intelligence is derived from human sources of information (the occasional wiretap notwithstanding).

E. LAW ENFORCEMENT ANTITERRORISM METHODS AND MEASURES

Properly collected and analyzed terrorist threat intelligence enables authorities to develop sound, focused security countermeasures. This thesis describes and evaluates intelligence techniques that domestic law enforcement officials can apply against Islamist transnational threats. These methods have primarily been extrapolated from U.S. Intelligence Community methods in overseas operations. Techniques must be tailored to the legal, political and social constraints of the domestic environment, and the capacities of the U.S. law enforcement community. Certain established practices, such as employing informants, straddle both intelligence and law enforcement and yield methods

[11] McCue, pp. 55-56, 58; Khalsa, pp. 3-4, 21.

that can be suited to antiterrorism. This thesis extrapolates from various terrorist case studies, to include those cases where such intelligence-based antiterrorist or counterterrorist methodologies have been used. The case studies include the attacks on the American embassies in Africa; the attack on the USS Cole in Yemen; the 9/11 attacks; and numerous attacks post-9/11, such as the Madrid and London rail bombings, and smaller incidents of pre-operational target assessment that were interdicted by police before an attack could materialize. Some offer insight into a very narrow portion of the terrorist methodology spectrum, such as a specific means of acquiring funds or elements of pre-attack reconnaissance operations. Nonetheless, a broad range of narrow case studies reveals certain operational and tactical patterns. Analyses of Al-Qa'eda and Islamist documents supplement the case studies, offering further insight into terrorist tactics and methods, while also placing them into a strategic and ideological context.

F. THESIS SYNOPSIS

Six chapters compose the thesis, which concentrates on the threat posed by transnational Islamist terrorism as influenced by al-Qa'eda's Salafist global jihad. The work begins with a presumption that the reader has a basic grasp of Islam and radical Islamic, transnational terrorism. Following this Introduction, Chapter II discusses the grand strategy of the global jihad, as well as the operational methods jihadi terrorists employ to facilitate their attacks. Since law enforcement intelligence primarily comes from human informants, and because human intelligence is uniquely suited to targeting terrorist operations, law enforcement antiterrorism intelligence best blends traditional police assets with intelligence community techniques. Thus, Chapter III considers how law enforcement officials can apply human intelligence collection strategies against transnational Islamic terrorism, with a consideration of the distinct functional roles officers must fulfill. Once intelligence has been collected in the field, the authorities must analyze it. Analysis, under-appreciated and neglected in both the law enforcement and intelligence communities, receives special attention in Chapter IV, since it represents the bedrock of good operational planning and sound security countermeasure development. The thesis concludes in Chapter V by examining risk assessment and security planning principles, and proposes a multi-layered evaluation methodology. The appendices provide more detailed information and practical examples of such concepts as

al-Qa'eda intelligence collection requirements, source recruitment strategies, or use of Chapter Five's proposed risk assessment methodology.

G. A NOTE ON SPELLING, RENDITION OF FOREIGN TERMS, AND DATE CONVENTIONS

Numerous foreign terms and names, principally in Arabic, appear in this work. Most terms are italicized, except for those that have become common in English usage, such as Islam, imam, mosque, jihad and jihadi. They have been adopted wholesale into the English vernacular, and are therefore treated essentially as borrowed words. Other terms of foreign derivation that have been Anglicized, such as the various "-isms" (Salafism, Islamism, or jihadism) are no longer purely foreign, and thus are treated as English words without italicization.

The thesis uses a consistent romanized spelling convention throughout the text. However, terms and names that appear in quotes or citations retain their original spelling. Thus, al-Qa'eda may be spelled as "Al Qaeda" or "al-Qaida." Similarly, the name Muhammad may appear as Mohamed or another variant. The same holds true for date conventions. This thesis uses the European day-month-year standard (e.g., 11 September 2001), but dates that appear in quotations or the titles of cited works remain in their original form. For example, the American date convention is retained when it is part of the title of a cited work such as, "Statement of Brian Michael Jenkins, Senior Advisor to the President of the RAND Corporation[,] Before the Senate Armed Services Subcommittee on Emerging Threats[,] November 15, 2001."

The term "9/11" is employed as a generally accepted shorthand for 11 September 2001 within the specific context of the terrorist attacks. Thus, references to "post-9/11" policies and the "pre-9/11" era provide a less cumbersome means to delineate periods of time that fall on either side of this pivotal date.

II. ISLAMIST TERRORIST METHODOLOGY

The current global jihad departs from the brands of terrorism the world saw during the 1970s, 1980s and early 1990s by virtue of its apparent worldwide nature and penchant for mass casualties. The wide incidence of Islamist terrorism arguably does not represent a monolithic, centrally controlled campaign. Nevertheless, the phenomenon bears certain identifiable hallmarks, particularly in methodology. These methodological threads, woven together, create a recognizable jihadi signature. Law enforcement and intelligence officials must study this methodological signature to guide their antiterrorism and counterterrorism planning.[12]

Al-Qa'eda, as the self-proclaimed vanguard of the jihad, would like to exert as much influence as it can on global operations.[13] Its degree of control varies across its constituency, but Islamist terrorists throughout the jihad have coalesced around some common operating principles which al-Qa'eda promulgated. Even as techniques evolve, the players share their discoveries and participate in a form of group learning. The methodologies that emerge represent the very threats law enforcement and intelligence officials endeavor to protect against.

Those who claim leadership of the global jihad, such as ideologues and strategists associated with al-Qa'eda, provide both strategic and tactical guidance for the movement. Tactics normally derive from strategic objectives and pronouncements, but al-Qa'eda recognizes that the various affiliates or "franchise" groups that join the global jihad bring their own parochial goals with them. Al-Qa'eda's leaders have crafted a strategic outlook

[12] *Antiterrorism* refers to defensive actions taken to protect against an attack, such target hardening. *Counterterrorism* consists of "offensive measures taken to interdict or respond to a terrorist act," like arrests of terrorist cells, or post-incident investigations. (See Joseph Autera, "Before It Makes the Headlines: Effective Threat Detection Strategies and Tactics," *Journal of Counterterrorism and Homeland Security Studies* (Fall 2003): 36.).

[13] Al-Qa'eda has accepted a diminished degree of direct control over many facets of the global jihad, "but there is also evidence of a structure that survives." Al-Qa'eda will not accept a complete devolution into a "leaderless resistance" movement, which "would reduce al Qaeda [*sic*] to mere exhortation." (Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves* [Santa Monica, CA: RAND, 2006], p. 34.)

that acknowledges these local agendas and gives the groups latitude to pursue them, but also strives to capitalize on their local efforts in support of its broader, global aims.[14]

A. STRATEGY AND VISION

Al-Qa'eda's overarching strategy incorporates both religious and political platforms. A fundamentalist Islamist organization normally would not distinguish between the two, as Islam is arguably a complete way of life that guides faith and government in tandem. Osama bin Laden is a shrewd politician, however, and undoubtedly recognizes that his constituency does not necessarily subscribe to the full *salafi* agenda. His public pronouncements, though peppered with religious rhetoric, levied political demands: an end to the American troop presence in Saudi Arabia, a reversal of U.S. support for Israel and the "apostate" Arab regimes, and a U.S. disengagement from Iraqi affairs.[15] Bin Laden's political objectives resonate with many in the Muslim world, though his religious agenda may hold less attraction.[16] Few would embrace a complete submission to an ultra-conservative, Taliban-style Caliphate.

1. The Strategic Plan

Politics may frame the short-term agenda, but a religious vision underscores the grand strategy. A seven-phase strategy for the global jihad publicly appeared in 2005. The work has been attributed to a high-ranking al-Qa'eda member, Muhammad Ibrahim

---

[14] Center for International Issues Research, "Al-Qaida's Global Strategy Part 4 of 5: Planning for the Future—Phases Four to Seven," *Global Issues Report* (6 October 2006): 4 [electronic document].

[15] Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama bin Laden*, First Touchstone Edition (New York, NY: Touchstone [Simon & Schuster, Inc.], 2002), pp. 226-227; Robert A. Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York, NY: Random House, 2005), pp. 54-55.

[16] Seyyed Vali Reza Nasr, lecture on Islamic fundamentalism at the Naval Postgraduate School, Monterey, CA, 27 September 2006; LTC Michael F. Beech, U.S. Army, "Observing al Qaeda through the Lens of Complexity Theory: Recommendations for the National Strategy to Defeat Terrorism," [*U.S. Army War College Center for Strategic Leadership*] *Student Issue Paper*, vol. 204-01 (July 2004): 12-14. Al-Qa'eda propaganda strategy dictates that most proclamations "should include [al-Qa'eda's] general goals which are acceptable to the people, [namely,] to get rid of the enemies of the Umma [i.e., America and the West] and their agents [i.e., the apostate regimes]." (Abu Bakr Naji, *The Management of Savagery*, translated by William McCants [{West Point, NY: Combating Terrorism Center} and {Cambridge, MA}: John M. Olin Institute for Strategic Studies, 23 May 2006], p. 47.)

Makkawi, known by his *nom de guerre* Makkawi as-Sayf al-Adel.[17] The seven phases follow a two-decade timetable with key milestones:[18]

- During Phase 1, "Awakening Phase," from 2000 to 2003, al-Qa'eda initiated its war with the United States.
- Al-Qa'eda is currently executing Phase 2, "Opening the Eyes Phase," from 2003 to 2006, where it hopes to establish an operating base in Iraq from which it intends to launch a wider campaign.
- In Phase 3, "Rising and Standing Up Phase," from 2007 to 2010, al-Qa'eda will strike Israel in the hope the international community will recognize al-Qa'eda as the leader of the worldwide Muslim community, or *umma*.
- Phase 4, "Rejuvenation Phase," from 2010 to 2013, is marked by a campaign to replace apostate regimes with Islamic governments. The war against the U.S. will intensify, with an emphasis on operations that will injure the American economy. Such attacks include computer network attacks and assaults on the petroleum industry.
- American hegemony and Israeli regional power will wane during Phase 5, "Announcing the Nation Phase," between 2013 and 2016, while India and China become the new world powers. The *umma* will announce the formation of the Caliphate (the "Islamic Nation").
- Phase 6, "Comprehensive Confrontation Phase," beginning in 2016, represents the grand the Caliphate conquers the West.
- Phase 7, "Final Victory Phase," begins in 2020 and lasts a maximum of two years. This phase marks the Caliphate's consolidation of power and rule over the entire Islamic world.

A similar work, written under the pseudonym Abu Bakr Naji, serves as a strategic manual for the global jihad. Published as a volume rather than an Internet-based document, *The Management of Savagery* represents a more scholarly work for a more

[17] Center for International Issues Research, "Al-Qaida's Global Strategy Part 1 of 5: Antecedents and Evolution," *Global Issues Report* (30 August 2006): 2 [electronic document]. His various aliases can be found at http://www.fbi.gov/wanted/terrorists/teraladel.htm (accessed 3 November 2006).

[18] The descriptions of the listed phases come from Center for International Issues Research, "Al-Qaida's Global Strategy Part 1 of 5," citing the following Arabic language jihadi web sites: "Strategy of Al-Qaida [original title in Arabic]," *Al-Ommh*, http://www.alommh.net/estra.htm (accessed 29 December 2005 and 5 January 2006); "Islamic Military Ideology [original title in Arabic]," *Al-Ommh*, http://www.alommh.net/forums/showthread.php?t=1629 (accessed 30 December 2005 and 5 January 2006); and "The Nation is Coming [original title in Arabic]," *Al-Ommh*, http://www.alommh.net/forums/showthread.php?t=1694 (accessed 30 December 2005 and 5 January 2006).

limited academic audience, replete with citations of other established Islamist ideologues.[19] A careful reading of the work suggests Abu Bakr may be closely tied to al-Qa'eda's senior leaders.[20]

The Management of Savagery places the global jihad into historical context, then plots a strategy for defeating the West (America and its allies) and the apostate regimes it props up in the Muslim world. The work includes general instruction on organizational management and operational planning for terrorist cells. Two principles permeate the strategy. First, the vanguard of the global jihad should seek under-governed regions rife with chaos ("region[s] of savagery," known in U.S. political vernacular as security vacuums), and move in to establish an Islamic order therein based on the *sharia*, similar to how the Taliban appropriated feudal Afghanistan after the Soviet withdrawal.[21] This echoes strategic aims that al-Qa'eda promoted since its inception; currently, al-Qa'eda hopes to create an Islamist base or "emirate" in Iraq after forcing a U.S. withdrawal.[22] Second, Abu Bakr advocates a protracted conflict with America and the West. The *mujahedin* should drain the enemy's resources through military engagement with American forces (most notably in Iraq) and asymmetric attacks on U.S. economic targets in a campaign of "vexation and exhaustion."[23]

2. Terrorist Warfare Evolving

Economic warfare plays prominently in both Naji's and al-Adel's pieces, and petroleum resources figure prominently in their respective target lists.[24] Naji's prose hints at a shift in how the global jihad may employ terrorism, and a number of other

---

[19] Center for International Issues Research, "Al-Qaida's Global Strategy Part 5 of 5: Comparison of Al-Qaida's Seven-Phase Strategy with 'The Management of Savagery,'" *Global Issues Report* (30 August 2006): 1-3 [electronic document].

[20] Ibid., p. 1.

[21] Naji, p. 11.

[22] Combating Terrorism Center, *Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities* (West Point, NY: Combating Terrorism Center, 14 February 2006), p. 48.

[23] Naji., pp. 16-21.

[24] Center for International Issues Research, "Al-Qaida's Global Strategy Part 5 of 5," p. 5; Naji, pp. 19-20, 21. Petroleum targeting is featured in other al-Qa'eda public discourse. In an al-Qa'eda videotape produced in September 2005, Ayman al-Zawahiri called for "strikes against [petroleum] infrastructure in the Persian Gulf region." See Fred Burton, "Al Qaeda: Targeting Guidance and Timing," *Stratfor*, 9 December 2005, http://www.stratfor.com/products/premium/read_article.php?id=259453 (accessed 18 February 2006).

Islamist pundits have embraced the new concept of "economic attacks."[25] Attacking targets ("particularly petrol" assets in the Middle East) to inflict economic damage will apply pressure to the United States, which in turn will squeeze its Arab allies for additional defensive measures.[26] Naji's treatise does include references to instilling fear in the enemy, but his discussion of economic attacks lacks any such allusion, suggesting al-Qa'eda may have added an element of axiological targeting[27] (striking assets which an enemy values instead of targets whose destruction would simply induce terror or impair military capability) to its operational repertoire.

Al-Adel's endorsement of cyberattacks highlights another digression from traditional terrorism. Al-Qa'eda hackers might disrupt an electronic commerce system or launch a denial of service attack, temporarily disabling part of a network, but such an attack would not constitute violence. While consumers may fear a financial loss resulting from the network shutdown, they would not likely feel the same sense of terror inspired by a major bombing.[28] Information system attacks would more closely resemble a form of harassment, certainly a valid component of asymmetric warfare,[29] though not terrorism *per se*. This suggests al-Qa'eda embraces a more complex campaign strategy.

3. Information Operations

Information operations and propaganda factor significantly in Al-Qa'eda's global campaign plan. Seized al-Qa'eda documents detail the organization's structure, which includes a Informational Committee charged with propagating "al-Qa'eda's vision of

---

[25] Center for International Issues Research, "Postings Cite U.S. 'Economic Weakness,' Call for 'Economic Jihad,'" *Global Issues Report* (27 September 2006): 1-3 [electronic document].

[26] Naji, p. 19.

[27] For a full discussion of axiological targeting, see Lt Col Peter W.W. Wijninga, Royal Netherlands Air Force, and Richard Szafranski, "Beyond Utility Targeting: Toward Axiological Air Operations," *Aerospace Power Journal* (Winter 2000): 45-59. One should note that Naji feels stifling America's access to petroleum has operational effects as well as economic ones, since a weakened economy has trouble sustaining a military campaign. It has the second effect of forcing The U.S. to divert resources to protect the economic assets, which reduces effective fielded troop strength and further drains the economy. See Naji, pp. 21-22.

[28] Maura Conway, "Terrorism and IT: Cyberterrorism and Terrorist Organizations Online," in *Terrorism and Counterterrorism: Understanding the New Security Environment*, eds. Russell D. Howard and Reid L. Sawyer (Guilford, CT: McGraw-Hill/Dushkin, 2004), pp. 273-275.

[29] Mao Tse-Tung, *Mao Tse-Tung on Guerilla Warfare*, translated and with an introduction by Samuel B. Griffith (New York, NY: Praeger Publishers, Inc., 1961), p. 102.

jihad to all Muslims."[30] Naji assesses that many young *mujahedin* lack a firm grounding in the jihad's religious and ideological principles, so the al-Qa'eda High Command—composed of leaders who are "disciplined intellectually—must "communicate [al-Qa'eda's directions to these youth."[31] Al-Qa'eda must also disseminate its message beyond the ranks of the *mujahedin* and reach the general public. Ideologue Mustafa Setmariam Nasar, alias 'Umar 'Abd al-Hakim, writing under the pen name Abu Mus'ab al-Suri, attributes the failures of past jihads to an inability to rally the masses. Imams (congregational clerics) need to play a role in firing up support in their congregations for the jihad, coupled with "aggressive media campaigns."[32]

A public media campaign figures prominently into the propaganda calculus. Naji argues that when the "hostile media" cover terrorist operations with opprobrium, "there is no way to justify the operations save by issuing public statements."[33] Furthermore, the Western media bring news of successful terrorist operations into "every home of the unbelievers," and thereby affect public opinion regarding Western activities in the Middle East.[34] Lastly, non-traditional media, such as the Internet, have become a pivotal component in the jihadi propaganda machine. The World Wide Web enables jihadi ideologues to reach a broad, global audience, particularly young Muslim adults who prefer the Internet as their primary news source over traditional print and broadcast media.[35] Al-Qa'eda boasts a sophisticated, Internet-savvy media branch, the Global

---

[30] Harmony Document AFGP-2002-000078, in Combating Terrorism Center, *Harmony and Disharmony*, p. 62.

[31] Naji, p. 59.

[32] Jarret M. Brachman and William F. McCants, *Stealing Al-Qaida's Playbook* (West Point, NY: Combating Terrorism Center, February 2006), pp. 15, 17. (The specific quote comes from the report's authors, not al-Suri. Also, the authors spell Nasar's middle name "Setmarian," but this appears to be a typographical error since multiple other sources spell it "Setmariam.")

[33] Naji, p. 47.

[34] Naji, p. 92.

[35] Bruce Hoffman, "The Use of the Internet By [*sic*] Islamic Extremists," *CT-262-1: Testimony presented to the House Permanent Select Committee on Intelligence on May 4, 2006* (Santa Monica ,CA: RAND, May 2006), p. 20, http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf (accessed 12 November 2006).

Islamic Media Front, which distributes jihadi multimedia productions to motivate and educate jihadis and sympathizers around the world.[36]

Al-Qa'eda's information dissemination apparatus does more than simply promulgate ideology and a broad vision. It bridges the strategic and tactical levels of the campaign, for the dissemination system actually provides specific guidance, education and training to *mujahedin* in the field, arming them with the tools, tactics and techniques necessary to prosecute the jihad.

B. TOOLS, TACTICS AND TECHNIQUES

Prior to 9/11 and the loss of its Afghan safe haven, al-Qa'eda promulgated operational skills and tradecraft through its training camps. Al-Qa'eda codified much of this material in an internal text it published for its trainees and operatives, entitled *Military Studies in the Jihad Against the Tyrants*, and known simply in the West as the *Al-Qa'eda Manual* or the *Terrorist Training Manual*.[37] The text covers, in detail, operational planning, intelligence collection, weapons construction and employment, logistics and security. Al-Qa'eda employed a top-down teaching and learning approach until 2001. Currently, with the al-Qa'eda core in hiding and geographically isolated from the minions in the field, learning in the global jihad has transitioned to a flatter form of information exchange using the Internet. Al-Suri extols the Internet's utility, for it can transform any Muslim household into a training camp, a recruiting center and a staging area for actual terrorist operations.[38] Jihadi sites have proliferated, and peer-to-peer information sharing has become the norm. Some higher-ranking experts and ideologues still promulgate top-down advice and direction, but they represent only one current of information flow among many.

---

[36] Center for International Issues Research, "Al-Qaida's Global Strategy Part 3 of 5: Phase 2 'Opening the Eyes' Implementation," *Global Issues Report* (6 October 2006): 3 [electronic document].

[37] *Military Studies in the Jihad against the Tyrants* [a.k.a. *The al-Qa'eda Terrorist Training Manual* or *The Encyclopedia of Jihad*], [attributed to Al-Qa'eda, ca. 1992 or 1993, translated by the Greater Manchester Constabulary, UK, ca. 2002].

[38] Combating Terrorism Center, *Harmony and Disharmony*, p. 54.

The Internet has fostered a form of distance learning for terrorists in the global jihad.[39] It enables geographically separated cells to communicate, exchange ideas and lessons learned, and share technical and tactical information in the furtherance of attack operations. Al-Qa'eda's Global Islamic Media Front even maintains an online training resource library.[40] Web interaction is difficult for authorities to detect and intercept by virtue of its lack of physical movement and the Internet's vast size.[41] This relative security, coupled with its accessibility, makes the Internet an ideal medium for jihadi collaboration.

1. Innovators or Imitators?

Shared learning and collaboration enable the global jihad because, methodologically, a terrorist will do tomorrow what worked for someone else yesterday. A cell will favor techniques similar to what other groups have employed, and will attack targets of the same type that other cells have successfully struck. Brian Michael Jenkins of the RAND Corporation notes that "[t]errorists tend to be imitative. One attack, when seen by terrorists as successful, inspires similar attacks. We need only to look at airline hijackings and subway bombings."[42] The Algerian Armed Islamic Group bombed a Paris subway as early as 1995, and suicide bombers drafted a plan to attack the New York City subway two years later.[43] The 11 March 2004 Madrid commuter train bombings were followed by the London suicide subway bombings on 7 July 2005. Fourteen days later that same month, another cell apparently tried to imitate the attack by striking the London

[39] Steve Coll and Susan B. Glasser, "e-QAEDA: From Afghanistan to the Internet—Terrorists Turn to the Web as Base of Operations," *The Washington Post* (7 August 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (accessed 4 November 2006).

[40] Ibid.

[41] Ibid.

[42] Jenkins, *Unconquerable Nation,* p. 161.

[43] Brian Michael Jenkins, "Statement of Brian Michael Jenkins, Senior Advisor to the President of the RAND Corporation[,] Before the Senate Armed Services Subcommittee on Emerging Threats[,] November 15, 2001," in *Terrorism: Current and Long Term Threats*, CT-187 (Santa Monica, CA: RAND, 2001).

subway again. Not only did the second group hit the same target set as the first (subway trains and a double-decker bus), they also mimicked the attack method, using explosives hidden in knapsacks.[44]

Terrorists borrow techniques from each other. For all the talk of terrorists being creative and adaptable, most are relatively formulaic. Behind every innovator, several imitators follow, and frequent imitation leads to proliferation. Vehicle-borne improvised explosive devices (VBIEDs) represent the archetype of modern terrorist weapons delivery, from car bombs in Colombia, to truck bombs in Saudi Arabia, to boat bombs in Yemen, to hijacked, fuel-laden airliners in America. Examples abound: the 1983 suicide truck bombing of the U.S. Marine barracks in Beirut, Lebanon; Timothy McVeigh's 1995 truck bombing of the Murrah Federal Building in Oklahoma City; the 1995 car bombing at the Office of the Program Manager-Saudi Arabian National Guard headquarters in Riyad in 1995; the 1996 truck bombing of the Khobar Towers U.S. Air Force dormitory in Dhahran, Saudi Arabia; the 1998 twin suicide car bombings of the American embassies in Africa; the suicide boat bombing in 2000 of the USS Cole in Yemen; and numerous car bombings in post-2003 Iraq. VBIEDs are effective because they hold a lot of explosives and are mobile, enabling terrorists to assemble the explosive device at their leisure, far from the target,[45] and then take it to the attack location when they are ready to strike.

---

[44] Yael Shahar, "London Underground Partially Shut Down after Minor Explosions," The Institute for Counter-Terrorism, 21 July 2005, http://www.ict.org.il/spotlight/det.cfm?id=1094 (accessed 5 November 2006); Don Philpott, "The London Bombings: New Evidence Points to Al-Qaida and a New Terror Campaign," *Homeland Defense Journal Special Report*, [2005], http://www.homelanddefensejournal.com/pdfs/LondonBombing_SpecialReport.pdf (accessed 5 November 2006); Fred Burton, "The Psychological Battlefield," *Stratfor*, 10 August 2005, http://www.stratfor.biz/Print.neo?storyId=253467 (accessed 18 February 2006).

[45] Al-Qa'eda apparently has a formula for the staging area as well. The operatives in Tanzania and Yemen selected very similar houses to construct their explosive devices: "a single-family house with high walls, a gate, and a compound area in a neighborhoods where no one could see what was going on inside the house and yard." (Bergen, p. 115.) A terrorist video of a VBIED assembly area in Chechnya depicts the same scene: The terrorists assembled the car bomb in a walled yard, attached to a house in a semi-rural neighborhood. (Video available at http://www.ogrish.com/archives/footage_of_car_bomb_blowing_up_near_army_convoy_chechnya_2001_Sep_12_2004.html [accessed 5 November 2006].)

Terrorists are persistent. The old adage fits: "If at first you don't succeed, try, try again."[46] Al-Qa'eda terrorists in Aden, Yemen, unsuccessfully tried to bomb the USS The Sullivans as it refueled in the harbor on 3 January 2000. The attempt failed when the operatives overloaded the attack craft with explosives and sank it.[47] The operatives regrouped and on 12 October attacked the USS Cole using a small, explosive-laden boat, killing seventeen U.S. Navy sailors.[48]

The 11 September 2001 attack on the World Trade Center most dramatically highlights the terrorists' patience and persistence. The 1993 bombing killed six and injured over a thousand people.[49] It did not collapse the towers, however, a point FBI Special Agent Chuck Stern made clear to Ramzi Yousef, the operation's chief planner, following his 1995 capture and extradition from Pakistan.[50] Unfortunately, al-Qa'eda rejoined with the most audacious terrorist atrocity in history—more than eight years after the first attempt—and destroyed both towers, killing thousands of people.

The 11 September attack clearly demonstrates the terrorists' patience, persistence and imitative nature. The fact Islamist terrorists re-engaged the World Trade Center was not a major surprise, in retrospect, since they had demonstrated their desire to strike it in 1993. Many people expressed shock, however, that the terrorists had used airliners as guided missiles, though the method actually had precedent. The Japanese pilots introduced the kamikaze technique during World War II to great effect. Terrorists have since dabbled with the concept over the years, though not with much success. A defector debriefing disclosed North Korea and Iran developed a kamikaze pilot training program in 1989.[51] They plotted to have a pilot fly an aircraft, loaded with explosives, into the White House. Authorities stifled a similar plot in Nepal, in which terrorists were

---

[46] Antiterrorism planners should not relax simply because a terrorist attempt on a given target, or target type, fails. The terrorists—or another sympathetic cell—may try to strike the target again, perhaps out of stubborn pride, or an effort to blunt U.S. arrogance in face of the initial jihadi failure.

[47] Bergen., p. 189.

[48] Ibid., pp. 171-172.

[49] Gerald Posner, *Why America Slept: The Failure to Prevent 9/11* (New York, NY: Random House, 2003), pp. 62-63.

[50] Ibid., p. 90.

[51] Joseph S. Bermudez, Jr., *Terrorism: the North Korean Connection* (New York, NY: Crane Russack [Taylor & Francis New York, Inc.], 1990), p. 83.

allegedly planning fly a hijacked airliner into a target, possibly in India.[52] In 1994, Armed Islamic Group terrorists took over an Air France passenger plane in Algeria with plans to explode it over Paris or crash it into the Eiffel Tower—until French commandos stormed the plane during a refueling stop in Marseilles.[53]

After 9/11, terrorists are unlikely to hijack a plane successfully and use it as a guided missile. The increased security measures, combined with a new passenger attitude, will stymie almost any hijacking attempt. In the event terrorists get aboard an airliner with weapons, the passengers will likely turn on the hijackers, as the passengers did on United Airlines Flight 93. Today, the latest scheme simply involves blowing up an airplane in mid-air. Richard Reid, a.k.a. Abd al-Jabbar, tried to do so with explosives smuggled in his shoes aboard a December 2001 flight from England to the U.S.[54] British authorities arrested a group of Islamic terrorists in August 2006 planning to board ten U.S-bound passenger planes with liquid explosives and blow the planes up during flight.[55] Do these examples represent terrorist innovation?

These operations hardly smack of originality. They have precedent, even before 9/11. Sikh terrorists secreted explosive devices onto two airliners on 23 June 1985; both devices exploded, one in mid-flight.[56] In a notorious example from 1988, Libyan agents placed an explosive device aboard Pan American Flight 103; the explosion destroyed the airborne plane near Lockerbie, Scotland.[57] Suspected Chechen "Black Widow" suicide

---

[52] Brian Michael Jenkins, "Statement of Brian Michael Jenkins..."

[53] Paul R. Pillar, "Fighting International Terrorism: Beyond September 11th," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 19; Gus Martin, *Understanding Terrorism: Challenges, Perspectives, and Issues* (Thousand Oaks, CA: Sage Publications, Inc., 2003), p. 236.

[54] Constable Steve Rocke, Peel Regional Police (Ontario, Canada), "Issues in Transportation Related [sic] Terrorism," International Counter-Terrorism Officers [sic] Association 3rd Annual Conference, Orlando, FL, lecture, 20 October 2005.

[55] John Ward Anderson and Karen DeYoung, "Plot to Bomb U.S.-Bound Jets Is Foiled: Britain Arrests 24 Suspected Conspirators," *Washington Post Foreign Service* (11 August 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html?referrer=email (accessed 3 October 2006).

[56] Constable Steve Rocke, Peel Regional Police (Ontario, Canada), "Terrorism & Attacks on the Civil Aviation Industry," International Counter-Terrorism Officers [sic] Association 2nd Annual Conference, Las Vegas, NV, lecture, 29 September 2004.

[57] Ibid.

bombers took down two Russian passenger planes on the same day in 2004.[58] The 2006 London trans-Atlantic plot not only followed precedent, but seems to have ridden on a recycled plan: Ramzi Yousef devised a scheme to blow up eleven airlines simultaneously over the Pacific in 1995.[59] Code-named "Operation Bojinka," al-Qa'eda shelved the plan, possibly because it was compromised when Yousef botched a separate operation in Manila, the Philippines. When he fled, he left behind a laptop computer that contained details on "Bojinka."[60] Still, despite the fact that counterterrorism officials around the world soon learned about this audacious plan, a new cell tried to bring it to fruition eleven years later. They were stopped, but if history is any guide, another cell will attempt a similar operation in the future. Terrorists are passionate recyclers.

2. Intelligence

Every operation, whether recycled or original, must be tailored to the unique circumstances presented by time and location. Al-Qa'eda stresses the role of intelligence in pre-operational planning. The *Al-Qa'eda Manual* has two chapters on espionage and intelligence gathering in which it outlines detailed collection requirements[61] (see Appendix A), advice for blending into a target society (along with religious justification for looking like an infidel while undercover),[62] and means by which to gather information. Methods include using open sources and the media,[63] recruiting informants,[64] interrogating abductees and hostages,[65] and physical reconnaissance and surveillance.[66]

Terrorists rely heavily on pre-operational surveillance to learn about their potential targets. The *Al-Qa'eda Manual* instructs operatives to sketch area maps of the

[58] Annie Jacobsen, "Russian Airliners Were Likely Exploded from their Toilets," *WomensWallStreet.com*, 30 August 2004, http://www.womenswallstreet.com/WWS/article_landing.aspx?titleid=76&articleid=748 (accessed 6 November 2004).

[59] Anderson and DeYoung; Posner, p. 88.

[60] Posner, p. 88.

[61] *Military Studies in the Jihad against the Tyrants*, pp. 72-73, 82-83, 85, 87, 89-91.

[62] Ibid., pp. 77-78.

[63] Ibid., pp. 80-83.

[64] Ibid., pp. 92-98.

[65] Ibid., pp. 78-79, 91-92.

[66] Ibid., pp. 85-91.

target's vicinity, and to photograph the target and its environs.[67] Prior to the 1998 attacks on the American embassies in Africa, "a local citizen reported seeing a man…videotaping the main gate of the Embassy compound" in Nairobi, Kenya.[68] Videotaping allows the surveillants to capture lots of imagery while recording vocal orientation on the audio, which proves especially useful if separate teams perform the surveillance versus the actual attack.[69] A photographic or video record familiarizes the attack team with the target and helps them identify it when they arrive in the area to do a final pre-attack assessment, operational rehearsal or the actual strike. Target *recognizability*—the ability to distinguish the correct target from other nearby facilities—is a critical factor in target assessment.[70] If authorities seize and review a videotape that focuses on distinctive markings, placards or signs on a facility in a way that appears to guide someone to that resource, the tape may represent a pre-operational surveillance record.

Surveillance on a static facility discloses its physical characteristics like the layout and construction. Terrorist planners normally require additional information about the activities at the facility, such as security protocols, traffic patterns or routine schedules. They may observe entry and exit procedures, shift changes at guard posts, or normal daily activity. They may also probe the facility by attempting to gain entry, or by phoning in a bomb threat and watching the response and evacuation procedures. The American Embassy in Nairobi received a number of bomb threats before the actual attack.[71]

Long-term surveillance necessitates prolonged and continuous visibility of the target. Al-Qa'eda operatives sometimes rent apartments overlooking the attack site. Ramzi Yousef and Khalid Sheikh Mohammed, future mastermind of the 9/11 attacks, plotted to assassinate Pope John Paul II during his January 1995 visit to the Philippines.

[67] *Military Studies in the Jihad against the Tyrants*, p. 90.

[68] Autera, p. 38.

[69] Vocal instructions were recorded by the videographer in a tape seized by Canadian authorities. The tape suggested the cell was advancing banks and subway stations as potential targets. (The video was presented by Constable Steve Rocke, Peel Regional Police [Ontario, Canada], "Understanding Terrorist Ideology," International Counter-Terrorism Officers [sic] Association 3rd Annual Conference, Orlando, FL, lecture, 18 October 2005.)

[70] U.S. Government Counterterrorist Training Group Special Seminar on Surveillance Detection, September-October 1997.

[71] Autera, p. 38.

Roughly a month before the visit, they and four other men took an extended rental in a hotel overlooking part of the Pope's motorcade route through Manila. (A fire in their room brought authorities to the scene and the perpetrators fled; the plot was thwarted by happenstance.)[72] Similarly, the team that plotted the 2000 operations against the USS The Sullivans and the USS Cole rented a house on a hilltop that gave them a clear view of ships refueling in the harbor of Aden, Yemen.[73]

3. Mass Casualty Attacks

Intelligence collection and detailed planning ultimately serve one objective: a lethal strike on the target. Mass casualty attacks are al-Qa'eda's hallmark, and the latest generation of terrorists are upping the ante.[74] RAND's Jenkins observes, "Body count appears to be the paramount criterion, outweighing any iconic value of a particular target—just about any crowded venue will do."[75] Naji argues sensational, high-casualty bombings draw media attention and amplify the enemy's sense of fear,[76] something Abu Musab al-Zarqawi and his ilk in Iraq have leveraged on the world media stage.[77] Al-Qa'eda encourages semi-autonomous affiliates to maximize the carnage—to a point. The younger generation's thirst for increasing bloodshed can have adverse political consequences down the road, upsetting al-Qa'eda's old guard.[78] Naji cautions newly emerging cells against pursuing an attack on the scale of 9/11, since an operation of that scope entails a degree of sophistication many smaller groups lack. Extremely large and ambitious attacks normally need the type of support only the al-Qa'eda core can provide, so such operations should first be vetted through the "High Command." He adds that planning a very large-scale attack risks diverting a cell's attention and resources from the numerous, smaller operations they could otherwise conduct to great effect. Younger,

---

[72] Posner, pp. 86-89.

[73] Bergen, p. 188.

[74] Center for International Issues Research, "Al-Qaida's Global Strategy Part 4 of 5: Planning for the Future—Phases Four to Seven," *Global Issues Report* (6 October 2006): 5 [electronic document].

[75] Jenkins, *Unconquerable Nation,* p. 36.

[76] Naji, p. 30.

[77] Center for International Issues Research "Al-Qaida's Global Strategy Part 4 of 5," p. 5 [electronic document].

[78] Jenkins, *Unconquerable Nation,* p. 100.

"nascent groups" should begin with more modest operations and solidify their proficiency before moving up to medium and large attacks.[79]

Multiple, smaller attacks have the benefit of draining the opponent's defensive resources. Repeated attacks on a particular target type, such as oil refineries or pipelines, highlight a continuing vulnerability in that sector. Likewise, if terrorists attack two targets of the same type "in a simultaneous operation in two different countries," then governments across the globe will feel compelled to protect all such targets in their respective countries. The "diversification and widening of the circle of targets…by small, separate groups" further bleeds the opponents in an ongoing "vexation" campaign.[80]

Al-Qa'eda introduced simultaneous attacks against geographically separated targets in 1998, with the attacks on the American embassies in Nairobi, Kenya, and Dar-es-Salaam, Tanzania. One version of the al-Qa'eda operations manual recommends striking four targets simultaneously (as on 9/11) in order to maximize the impact on the Western opponent,[81] which suggest al-Qa'eda grasps Westerners' concept of time. Punctuality and synchronization have a sharp impact on the Western psyche, for they imply the adversary (al-Qa'eda) has tremendous efficacy in planning and coordinating actions, without geographic limitations. Traditional Middle Eastern concepts of time and punctuality do not conform to Western cultural norms. An appointment for "the evening" is often sufficient in the Middle East; a precise meeting time of five o'clock may be unnecessary.[82] Al-Qa'eda has shown it is unrestrained by its own cultural paradigms,

---

[79] Naji, p. 17. The key Al-Qa'eda leaders seem to have self-imposed limits on casualties. Ramzi bin al-Shibh, one of the chief planners of the 9/11 operation, had begun drafting "The Truth About the New Crusade: A Ruling of the Killing of Women and children of the Non-Believers." Coalition forces in Afghanistan recovered the document from a captured computer. The unfinished treatise insisted on reciprocity (echoing Western Just War theory) and limited the number of casualties at "four million [dead] non-combatants, or…ten million of them homeless." (Alan Cullison, "Inside Al-Qaeda's Hard Drive," *The Atlantic Monthly* (September 2004), http://www.theatlantic.com/doc/200409/cullison (accessed 3 November 2006.)

[80] Naji, p. 19.

[81] Bruce Teft, "Terrorism Awareness—Islamic Terrorism: Origins and Prevents," International Counter-Terrorism Officers [sic] Association 3rd Annual Conference, Orlando, FL, lecture, 18 October 2005.

[82] Training Seminar by First Technologies, LLC., "Understanding Islamist Militant Terrorism and Prevention Strategies," Federal Law Enforcement Training Center, Glynco, GA, 16-17 September 2004.

and can employ Western concepts against its opponents to achieve a psychological advantage—almost a form of psychological *jujitsu*.

Suicide attacks add another dimension to the mind game. Suicide terrorism exacts a high cost on the perpetrator, a fact that illustrates the terrorists' resolve to the opponent. Staged against a backdrop of religious devotion, suicide attacks can signal the terrorists' affiliation with a larger, presumably sympathetic, religious constituency. From this constituency the target (the West) will see a pool of additional potential recruits, which induces the target to anticipate additional future attacks.[83] Al-Qa'eda undoubtedly hoped to capitalize on this psychological effect in its suicide attacks of 1998 (U.S. embassies in Africa), 2000 (USS Cole) and 2001 (9/11). The withdrawal of al-Qa'eda's central core into hiding post-9/11, however, has foisted "operational planning [onto] the operatives themselves...[who] are willing to sacrifice their lives, but not to waste their sacrifice. That pushes planners toward safe bets—easy targets," using less sophisticated operations.[84]

Perhaps the most frightening attack would be one involving weapons of mass destruction, or WMD. Analysts and politicians have expressed great concern about al-Qa'eda or its affiliates employing radiological bombs ("dirty bombs"), chemical agents or biological weapons. Coalition forces in Afghanistan discovered traces of chemical and biological agents at captured al-Qa'eda compounds; additional evidence obtained by military forces and journalists includes training materials and videotapes of gas testing on dogs.[85] Ironically, al-Qa'eda's efforts to develop an unconventional weapons capability appear to have been in response to America's fears about possible terrorist WMD use. Bin Laden's deputy, Ayman al-Zawahiri, sent an e-mail to Muhammad Atef in April 1999, in which he stated, "Despite their extreme danger, we only became aware of [WMD] when the enemy drew our attention to them by repeatedly expressing concerns

---

[83] Pape, pp. 28-29.

[84] Jenkins, *Unconquerable Nation*, pp. 83-84.

[85] Jonathan Spyer, "The Al-Qa'ida Network and Weapons of Mass Destruction," *Middle East Review of International Affairs*, vol. 8, no. 4 (September 2004): 34-35, http://meria.idc.ac.il/journal/2004/issue3/spyer.pdf (accessed 4 November 2006).

that they can be produced simply with easily available materials…"[86] A number of known or suspected al-Qa'eda proxies have attempted to conduct WMD attacks after 2001, but have been thwarted by authorities. In June 2002, authorities arrested Jose Padilla, who was suspected of building a radiological bomb for an attack in the U.S. Authorities in Thailand foiled a suspected cesium-137 radiological bomb plot in June 2003. An alleged chemical bomb attack against the Jordanian General Intelligence Department headquarters in Amman was also stymied in April 2004. Finally, police in August 2004 apprehended members of a cell in London with technical information on chemical weapons and pre-operational planning data on potential targets.[87]

The number of attempted WMD uses is low when compared to conventional explosive attacks. Al-Qa'eda's use of WMD, for the most part, seems to be restrained by a political calculus. The central organization "employs violence for clear political aims"[88] as outlined in its grand strategy, and it endeavors to corral the outlying affiliates within approved parameters as much as possible. Just as al-Zarqawi's ruthless beheadings in Iraq drew censure from the general Muslim public,[89] indiscriminate WMD attacks could damage al-Qa'eda's (and the overall global jihad's) political capital. This may be why Al-Qa'eda refuted allegations that the 2004 plot in Amman involved chemical agents.[90] Ramzi bin al-Shibh, one of the architects of the 9/11 operation, gave a secret interview to Arabic media outlet al-Jazeera, during which he noted al-Qa'eda had aborted a strike on a nuclear power plant because the planners could not gauge the ultimate outcome—an outcome with potentially disastrous consequences.[91] Similarly, releasing a biological contagion could backfire and undermine support for the jihad. Given today's global interconnectedness through international travel and trade, terrorists

[86] Ayman al-Zawahiri, Electronic correspondence to Muhammad Atef [translated], 15 April 1999, in Cullison.

[87] Spyer, pp. 36, 37, 38-39.

[88] Ibid., p. 34.

[89] Ayman Al-Zawahiri, Letter to Abu Musab al-Zarqawi [translated], 9 July 2005, http://www.weeklystandard.com/Content/Public/Articles/000/000/006/203gpuul.asp (accessed 31 May 2006).

[90] Spyer, p. 36.

[91] Magnus Ranstorp, "Statement of Magnus Ranstorp to the National Commission on Terrorist Attacks Upon the United States March 31, 2003," http://www.allamericanpatriots.com/m-wfsection+print+articleid-760.html (accessed 4 November 2006).

can expect a disease to spread to many countries, including those with populations sympathetic to al-Qa'eda. Jenkins asserts, "The crowded cities of Asia, the Middle East, and Africa, with their much weaker public health systems, are far more vulnerable to a pandemic than are American towns and cities….Contagious diseases…can only be initiated, not confined."[92] Al-Qa'eda, with its astute appreciation for propaganda and public relations, will most likely employ any weapons of mass destruction cautiously, ensuring their use furthers the long-term objectives of the global jihad.

C. LESSONS FOR ANTITERRORISM OFFICIALS

What should law enforcement and intelligence officials take from this overview? They should recognize al-Qa'eda's strategic roadmap for the global jihad, and how the jihad's strategic apparatus translates to tactical terrorist operations. Although al-Qa'eda's High Command may have physically withdrawn into hiding, leaving much more of the burdens for planning and execution on local affiliate cells, the Internet allows al-Qa'eda to maintain a degree of contact with them and provide them ideological and operational guidance. The Internet, by allowing far-flung cells to share ideological, operational and technical information, actually draws many of them into the parameters of a recognizable *modus operandi* (method of operation, or MO). Disparate terrorist cells have routine access to al-Qa'eda strategic indoctrination materials, and their collaborative nature encourages them to use familiar tactics against like targets, thus shaping a general pattern that law enforcement and intelligence analysts can evaluate and exploit in crafting defensive measures.

The web-based "electronic jihad" represents a powerful enabler for jihadi cells, but it also exposes them because of the web's open nature. Jihadis simply rely on the Internet's size to hide anonymously amidst millions of licit users. If antiterrorism officials partner with media and Internet watchdog groups, they can get leads on which sites the jihadis use. An undercover informant who has already tapped into the electronic jihad can provide specific URLs (uniform resource locators) that are kept close-hold in jihadi circles. Staying abreast of the web chatter, antiterrorism officials can monitor ideological threads, al-Qa'eda targeting directives, and tactical trends. Law enforcement and intelligence officers can use the anonymity that the Internet provides to insert

[92] Jenkins, *Unconquerable Nation*, p. 140.

themselves undercover into the “electronic jihad,” pretending to be sympathizers or up-and-coming terrorists themselves. From there, they can gather intelligence about specific plots, or develop sting operations.

Antiterrorism officials ultimately must stay abreast of terrorist strategy, tradecraft and targeting. As the terrorists attempt to guide each other in prosecuting the global jihad, they inadvertently share that guidance with the antiterrorism specialists. This forms the baseline for the authorities’ task of intelligence collection and exploitation.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE JOY OF HUMAN INTELLIGENCE: ITS UNIQUE APPLICATION TO HOMELAND SECURITY AND ANTITERRORISM

Law enforcement agencies routinely gather and evaluate information to investigate crime and accidents, monitor trends, and curb ongoing criminal activity. Some information rightly constitutes intelligence, since police collect it and assess it using a systematic process in order to derive conclusions about a particular subject of inquiry. The law enforcement community traditionally associated intelligence with narcotics or gang enforcement operations, but today's growing terrorist threat places an even heavier demand on police intelligence. Methodologically, the police can fulfill that demand using the same tools they apply to other criminal intelligence operations. Police derive much of their intelligence from people—human sources of information.

A. EMERGING ROLES IN PREVENTIVE POLICING THROUGH INTELLIGENCE COLLECTION AND EXPLOITATION

The American public has always relied on police at all levels to curb criminal activity and preserve a safe environment. Naturally, the success of police efforts varies over time and location. Only recently, however, has the criminal opponent posed such a formidable threat to the very security of our nation. For our nation's police, the coordinated transnational terrorist attacks on September 11, 2001 represented a change in criminal targeting; they were more akin to a military act of war, aimed at hobbling a nation, than a violent act perpetrated to further a criminal pursuit of profit. True, the United States has had few mass casualty terrorist events on American soil—Oklahoma City and the first World Trade Center bombing in 1993; but the scale of the attacks, coupled with their narrow scope, made them tragic anomalies in our relatively secure history. The scope of the al-Qa'eda attacks, however, has revealed them to be part of a broader campaign than any America has encountered at home before. The planning and targeting continue, and the public—the constituents of our law enforcement agencies—demand that the police rise to the challenge and mitigate the threat head-on. Our public servants at all levels—local, county, state and federal—must adopt a common set of law enforcement *roles* aimed at gathering, analyzing and using *intelligence* to prevent the next terrorist event, rather than merely investigating the last attack.

When people talk about "roles" in the war on terrorism and homeland security, they most often mean *agency* or *department* functions. The nation charges the Central Intelligence Agency and the other various intelligence organizations with identifying and locating terrorists abroad, and detecting their plans to attack American interests in advance. The military is responsible for striking the enemy on his home turf and rooting out the threat far from our shores. The Federal Bureau of Investigation works to uncover terrorists who have slipped past the first two groups and made it through the borders in the final stages of their targeting—or "home grown" terrorists of U.S. residency who already live in the country. Unfortunately, the state, county and local police often find themselves left with incident response—when all others have failed to prevent an attack from happening, our police officers, EMTs and firefighters are left to clean up the mess. While these roles are valid, they cannot be the sole model by which we frame our homeland security posture. It is more useful to examine *functional* roles, which are not restricted to specific agencies, as a mechanism to harness the country's organic capabilities to fight terrorists on our home soil. Those roles, properly integrated, can help law enforcement develop and use *intelligence* to secure America.

Intelligence is the key to gaining ground against the terrorists. The public isn't so much interested in a post-incident investigation that fixes blame for terrorist activity to a given group. While that is important from a justice—and perhaps a deterrence—perspective, preventing terrorism in the first place is paramount. Military planners and law enforcement officers alike understand the value of advance information when it comes to proactive operations. Much like a raid on an enemy military compound, a police raid or proactive bust relies heavily on advance intelligence for success. The intelligence may come from a variety of sources: area casing and reconnaissance, confidential informants, trash covers, mail covers, wiretaps or undercover officers. The police use the same techniques as intelligence agents; they simply use them in a different environment, within different legal guidelines, and against different targets. Those police agencies that excel in gathering and exploiting criminal intelligence can attribute their crime fighting success to the roles they employ in that endeavor. Often one group of officers handles the informants, while others analyze the gathered intelligence, and still

others specialize in the actual operation. In smaller departments, officers fill multiple roles, but the roles can nevertheless be viewed as distinct.

The first is the role of the uniformed police officer, or for the sake of discussion, the *patrolman*. This is the uniformed cop who walks a beat, rides a patrol, or mans a fixed post. The patrolman is the visible authority figure in society. Most often the patrol officer first receives reports of suspicious activity or an actual crime. In addition to being the obvious "go-to" officer for the neighborhood citizens, the patrolman enjoys an intimate familiarity with his or her duty post. The patrolman knows all the players, good and bad, and all the games on the beat. If a new player slips into town, the patrolman should know it. It's the patrol officer who can best detect when something's amiss. The key to detecting pre-operational terrorist activity is to know the daily norm, and to notice when something arises that doesn't belong.

The next role is that of the *agent*. Officers filling this role are the plain clothed police: the special agents, the investigators and the detectives. Their job is to bridge the gap between the uniformed officers and intelligence analysts. An agent typically conducts interviews, runs source and informant networks, and digs up bits of information that he can piece together to track down criminals and criminal activity. In the context of this thesis, it means terrorists and their operations.

The third role is that of the *analyst*, who is responsible for collating and analyzing raw data from the field. The analyst is expected to draw predictive conclusions from the evaluated data. In other words, the analyst helps law enforcement anticipate the enemy's next move. The analyst may reside at any level of law enforcement—federal, state, county or local. Analysts at different levels have access to different raw data within their respective jurisdictions, but they must all share with each other, laterally and vertically, to make sure they and their officers on the street see how their respective agencies and jurisdictions fit into a larger picture or context—regionally, or in some cases, nationally or internationally.

The three roles interact in a cycle (see Figure 1) wherein they gather and exploit intelligence. The patrolman *observes* his environment and collects basic threat information. The agent can also make passive observations, but focuses most of his

energy actively collecting information and applying low level analysis to it. The analyst gathers together information reported from the patrolman and agent in the field and systematically *analyzes* it. The analyst devises patterns and predictions of terrorist behavior, generating new information in the form of *finished intelligence* which can be sent out to the field to focus future observation and collection.

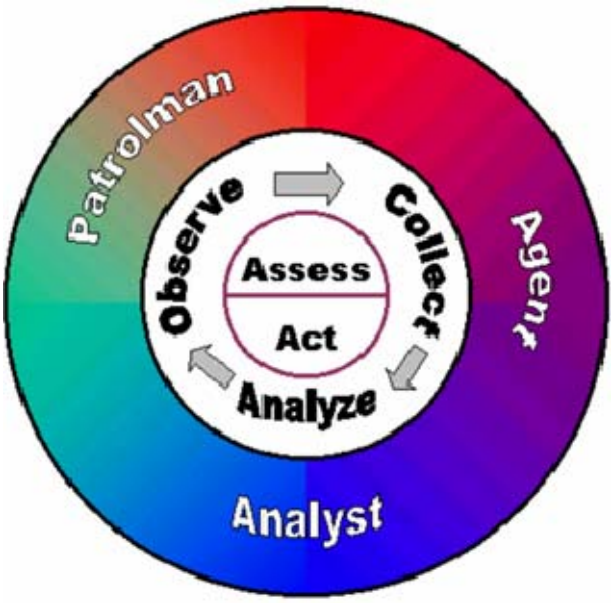

Figure 1 Law Enforcement Intelligence Roles

In each phase of the cycle, the various participants must *assess* the information they have gathered, developed or received—that is, determine its importance within the context of their respective roles and environments—and *act* appropriately based upon that assessment. Such action can include sharing information with other participants, to investigating suspicious activities, to making an arrest or to instituting defensive antiterrorism countermeasures.

B. HUMINT IN LAW ENFORCEMENT

The art of intelligence and spycraft predates the first reconnaissance satellite by several thousand years. Ancient intelligence derived from human sources. Even today, different agencies and different disciplines, from police to intelligence agencies to journalists, still use this common source of information—namely, people—though they may call them by different names: "sources," "informants," "spies," "agents," or "assets." It all constitutes human intelligence, or HUMINT.

HUMINT is uniquely suited to ground-level collection on terrorists. HUMINT can "look where the most sophisticated imaging satellite cannot begin to see—inside the human soul."[93] A well-placed human source can provide insight into an adversary's preconceptions, motivations, and intentions, engendering predictive intelligence. Technical collection platforms won't forecast terrorist attacks. Also, "[m]ost of the terrorist preparations that matter occur not in camps in the countryside of some place like Afghanistan, but in apartments in places like Beirut, Hamburg, New Jersey, or Florida."[94] Imagery cannot zero in and identify terrorists in dense urban environments; furthermore, disposable cell phones, human couriers, coded talk and commercial encryption complicate technical collection on terrorist communications.[95] An organizational insider, however, can provide detailed information on group membership, structure, location, capabilities, weaknesses and plans—the very things a terrorist organization labors to keep secret.

Human intelligence (HUMINT) represents a staple of law enforcement intelligence collection, particularly in proactive operations. Just as human informants play a key role in proactive narcotics operations, so, too do they in antiterrorism and counterterrorism efforts. HUMINT is a critical component in a terrorism prevention program, for it uncovers indicators of a terrorist presence in a given jurisdiction, information about specific terrorist personnel in the area, and clues about local terrorist activity. A multi-layered collection approach can offer authorities a variety of sources with complementary access to information and placement vis-à-vis terrorists and their support apparatus. Many of these potential sources, it should be noted, hail from specific ethnic and religious communities, by virtue of the Islamist jihadi threat on which authorities focus their collection efforts. The unique demographic dimension necessitates collectors to exercise a degree of cultural savvy in finding, recruiting and handling such

[93] Ralph Peters, "The Case for Human Intelligence," *Armed Forces Journal* (July 2005): 26.

[94] Paul R. Pillar, "Fighting International Terrorism: Beyond September 11th," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002), p. 23.

[95] Mark V. Kauppi, "Counterterrorism Analysis 101," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002), p. 43.

sources. Careful, planned source handling will afford police unmatched access to information on terrorist activity and plans in their area, enabling them to unravel any plots and thwart a future attack.

C. LOOKING FOR CLUES—JUST WHAT ARE WE LOOKING FOR?

Intelligence supporting antiterrorism programs has one primary purpose: preventing a terrorist attack.[96] Intelligence information may also assist in post-incident investigation and prosecution, but today's emphasis underscores prevention. Even post-incident information, while fulfilling evidentiary requirements for the prosecutorial case, should simultaneously feed analytical efforts to forestall the next attack.

Field collectors perform a proactive threat detection function for the analysts, seeking information that points the analysts to future terrorist operations. Terrorist cells, particularly those in targeted countries, are naturally secretive. Terrorist operatives nevertheless emit certain clues to their presence and their activities will display a distinct, though perhaps subtle, signature. These activities alert analysts to potential terrorist operations and are called *indicators*: both requisite and likely occurrences that one could observe as a terrorist "scenario unfolded." [97]

Conversely, an *indication* is something that has already happened that fits into an indicator category. In other words, an indication suggests the scenario has already manifested itself.[98] Analysts use *indicators* to predict the likelihood a single act might occur, while they employ *indications* to develop patterns and trends concerning multiple events. Proactive, preventive law enforcement and intelligence operations focus on indicators. Authorities must seek and recognize indicators of a terrorist organization's presence in their jurisdiction, for the terrorist network members themselves, and for their activities.

---

[96] Kauppi argues more specifically that a terrorism analyst's primary job is to forecast future attacks, thereby implying prevention. See Kauppi, p. 39.

[97] James J. McDevitt, "Summary of Indicator-Based-Methodology," unpublished handout, n.p., n.d., provided in January 2002 at the Joint Military Intelligence College, cited in Captain Sundri K. Khalsa, USAF, "Terrorism Forecasting: A Web-Based Methodology," *Occasional Paper Number Eleven* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004), p. 9.

[98] Khalsa, p. 13.

1. Indicators of Terrorist Presence

Authorities must first determine if terrorists themselves have appeared in their jurisdiction. In the case of Islamist terrorists, how might one know if jihadis or al-Qa'eda affiliated cells are present in a given area? Generally the first clue is "talk about town" concerning a particular Salafist group, often centered around key clerics or dynamic, vocal and charismatic informal leaders who openly espouse Salafist or jihadist beliefs. Vocal members of the community, preaching violent, anti-western rhetoric or espousing global jihad serve as a clear sign of a militant element in the community. Another clue to Salafist influence would be if people in the community begin taking on traditional Salafi ways, such as traditional dress and grooming (beards),[99] because Salfists are first and foremost Salafi.

The best sources to identify a Salafist cell would be moderate, non-Salafist Muslims who consider this subset of their community an unwelcome addition. Marc Sageman suggests finding sources in the fundamentalist Muslim community where Salafist sub-groups are likely to emerge.[100] More moderate Muslims, to include clerics, may find this militant bent disruptive. Salafists sometimes taut their religious superiority, lording it over the other "less devout" Muslims in the community; the Salafists may chastise them for their lack of devotion to the true path of Islam as Muhammad intended it to be. (Not surprisingly, the Arab *mujahedin* in Afghanistan alienated themselves from many Afghans because they regularly derided the Afghans as impious Muslims.)[101]

2. Individual Terrorist Network Members

Besides spotting Islamist or Salafist enclaves, one can further identify individual terrorist members by working the *association chain*. It may be possible to find terrorists by identifying potential associates first and working toward the hardened operatives. The associates are not necessarily members of the Islamist or Salafist clique themselves, or even witting supporters of the terrorist cell. Some of them are friends; others are relatives; still others are people who live or work in close proximity to the operatives and

[99] Marc Sageman, *Understanding Terror Networks*, Philadelphia, PA: University of Pennsylvania Press, 2004, p. 177.

[100] Ibid., p. 182.

[101] Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama bin Laden*, First Touchstone Edition (New York, NY: Touchstone [Simon & Schuster, Inc.], 2002), p. 68; Fawaz A. Gerges, *The Far Enemy: Why Jihad Went Global* (New York, NY: Cambridge University Press, 2005), pp. 82-83.

are in a position to observe them and pinpoint any behaviors or activities indicative of terrorist affiliation. These might include landlords, delivery people, maintenance workers, neighbors, shopkeepers or fellow mosque congregants.

Possible inroads to the association chain can also come from immigration screening whereby people with certain travel histories are flagged. Immigration inspectors should scrutinize people entering the country who have logged travel to a number of "hot" nations where global Islamist terrorists have concentrated or been active, such as Afghanistan, Indonesia, Malaysia, the Philippines, North Africa, Egypt, the Arabian Peninsula, the Caucasus region, Pakistan, Iran, France, Spain, Germany, Canada[102] or England.

Immigrations intelligence analysts can take these flagged travelers and cross-reference the information they provided on their immigration declaration forms with that of other flagged travelers. These forms should list their home addresses as well as their intended destination address in the United States. Immigrations officials can question the travelers during secondary screening, while also gathering information from their passports, airline tickets and receipts, and other travel documentation. Any personal references or business references the travelers offer during secondary screening also join the data pool. The analysts can cross-reference all of the data, from addresses to travel histories to names, against the data from their traveling companions and against information in standing databases. The analysts can perform link analysis to see if any common names, addresses, telephone numbers, or travel histories pop up as suspicious or unusual. Do different flagged travelers list the same references or addresses? Are any of their data elements linked with other noteworthy data in the databases? Subsequently, anybody these flagged travelers contact in the U.S. should be considered "of interest" (not *suspicious* or *guilty by association*) and earmarked for closer observation or investigation by authorities.

[102] Given the volume of cross-border traffic between the United States and Canada, flagging visitors merely on this travel criterion may prove unproductive.

Such link analysis can identify terrorists. Heather MacDonald of the *City Journal* notes:

> Had a system been in place in 2001 for rapidly accessing commercial and government data, the FBI's intelligence investigators could have located *every single one* of the 9/11 team once it learned in August 2001 that al-Qaida operatives Khalid al-Midhar and Nawaq al-Hazmi, two of the 9/11 suicide pilots, were in the country. By using…link analysis…investigators would have come up with the following picture: al-Midhar's and al-Hazmi's San Diego addresses were listed in the phone book under their own names, and they had shared those addresses with Mohamed Atta and Marwan al-Shehi (who flew United 175 into the South Tower of the World Trade Center). A fifth hijacker, Majed Moqed, shared a frequent-flier number with al-Midhar. Five other hijackers used the same phone number Atta had used to book his flight reservations to book theirs. The rest of the hijackers (who crashed in Pennsylvania) could have been tracked down from addresses and phones shared with hijacker Ahmed Alghamdi [who was in the U.S. on an expired visa].[103]

Authorities can also identify individual terrorists by investigating suspected organizational activities. Naturally, the people engaged in said activities will be associates or actual members of the network. Like any narcotics operation, where the street dealers and mules have a lesser investment in the criminal organization than the kingpin drug lords, low-level terrorist operatives—those acquiring funds and materiel or providing logistical support—will have less knowledge of the overall terrorist organization and plans than the key leaders. In fact, some peripheral supporters may not even recognize their link to a terrorist enterprise. Nevertheless, these people are connected ultimately to the core, and investigators can work their way along those links, deeper into the terrorist organization.

3. Indicators of Terrorist Activity

Terrorist activity displays several signatures, depending on the activity's specific nature. U.S. intelligence analysts interpolate indicators from field reports on such things as terrorist training, pre-operational surveillance of targets, tests of security at targeted facilities, terrorist travel patterns and travel data on specific individuals, and the movement of terrorist weapons and materiel.[104] These activities reflect pre-operational

[103] Heather MacDonald, "What We Don't Know Can Hurt Us," *City Journal*, 20 April 2004, http://www.city-journal.org/html/14_2_what_we_dont_know.html (accessed 17 February 2006).

[104] Khalsa, p. 9.

(pre-attack) preparations. Discerning indicators from more strategic, long-term preparatory actions requires an eye for subtlety.

Early stages of forming cells and support networks are less apparent than pre-operational targeting and planning. The formation of terrorist support networks and small cells tends to stay within the Muslim community, offering few indicators to the general public, while target assessment and later planning stages require the operatives to venture forth into the public at large, where their potential targets are.

The early phases of group formation are the hardest to detect, but afford law enforcement officials more time to collect information on the groups as the threat of actual attack is not imminent. As mentioned earlier, one indicator is the emergence of Salafist cliques within the Muslim community—young men who often isolate themselves from family, old friends or associates in favor of the new, religiously zealous clique. Groups of Salafists may reside together and share an apartment or house, focusing their lives on this new way of life emulating the *salaf*. For many, this may be the extent of their activity, and they may never make contact with actual terrorist cells. Some of these groups, however, may inquire into joining the jihad; they ask around the community looking to find someone with links to the global jihad network. Such links may be found with outspoken individuals professing jihad or telling war stories from regional jihadi struggles in Afghanistan, Chechnya, Iraq or the Philippines.

Ongoing terrorist cell activity includes fund-raising efforts. Most often these occur below the radar, and only recently have law enforcement organizations started to scrutinize seemingly innocuous fund-raising and charitable activities for potential connections to terrorist organizations. Press reports have highlighted the connections between a number of Muslim charities and Islamist terrorist organizations. These so-called charities serve as financial fronts to collect money from Muslims and funnel it to terrorist groups. Some of the contributors remain unaware their donations are destined for terrorist operations; others are keenly aware of the scam and consciously support it, knowing full well where their funds are headed.[105]

[105] John Roth, Douglas Greenburg and Serena Wille, *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission* [Washington, DC: U.S. Government Printing Office {electronic document}, 2004], pp. 21-22.

Local collections at the mosque, much like Sunday service collection in church, are commonplace. Where the money actually goes once collected, however, remains the chief cleric's purview. The mosque imam normally enjoys full discretion over the disbursement of the congregation's contributions. The community entrusts the imam to use the tithes (the *zakat*) to aid the poor, as this is a traditional responsibility levied upon Islamic clergy. But, if the imam has ties to Islamist groups, he may send money to them, with little transparency to his congregants.[106] The authorities must identify outspoken, radical imams who have suspected sympathies for terrorist organizations—or familial ties to known members of the organizations—and investigate their financial activities.

Criminal enterprises that implicate Muslims or Middle Eastern immigrants[107] require closer inspection, with an eye toward where the profits ultimately go. Investigators have often considered such schemes nothing more than economic crimes of greed, without considering their potential role in a larger, organized terrorist fund-raising apparatus. Seemingly petty operations may only bring in small sums within any one given jurisdiction. Similar or identical schemes, however, may have been established in numerous areas around the country, all funneling their small profits to a central collection point. A careful criminal intelligence assessment of these activities should identify any such connection.

Intelligence specialists must perform link analysis between the criminal suspects across the country to uncover connections or commonalities between them and their activities. Do they come from the same part of a given foreign country, or have they lived in the same U.S. city at some time in the past several years? Do they have a common address in their residence history? Do they use the same wireless phone company or Internet service? Who owns each store or business that's serving as the front? The stores may all title back to one owner or one family in another state. The

---

[106] Training Seminar by First Technologies, LLC., "Understanding Islamist Militant Terrorism and Prevention Strategies," Federal Law Enforcement Training Center, Glynco, GA, 16-17 September 2004.

[107] Criminal enterprises linked to the jihad may include smuggling tax-free goods into high-tax markets; production and distribution of counterfeit goods or bootlegged music and videos; resale of expired food products at small grocery or convenience stores; sale of stolen property; low-level fraud; credit card fraud and identity theft; international narcotics trafficking; and a host of others. (Drawn from the author's education, training and information-sharing with professional colleagues.)

businesses may bank with the same financial institution, or make financial contributions (think corporate tax deductions) to a common Islamic charity or scholarship fund.

Routine criminal investigations may thus yield information relevant to antiterrorism operations and investigations. Police additionally should expect to collect terrorism-specific information and generate leads outside of criminal inquiries, directly from managed human sources.

D. TYPES OF HUMINT AVAILABLE TO LAW ENFORCEMENT – THREE LAYERS

Law enforcement officials cannot situate themselves everywhere to spot criminals and terrorists. Human source networks provide the extended range authorities need to keep watch for terrorists and their activities. Police use human informants as a staple law enforcement tool. This familiar concept boasts deep roots in the profession, only a new target has emerged, requiring a slightly modified set of human sources. (Appendix B provides examples of various human sourcing operations.)

Citizens will have varying degrees of placement on the streets and in the community, and they will enjoy access to different types of information regarding terrorist operations. A layered approach to developing source networks, or *sourcing*, can give authorities information from broad, general indicators of terrorist presence, all the way down to details regarding specific cells and operational activities. The three layers consist of (1) a public awareness campaign soliciting the public at large to report suspicious activity; (2) open contacts networks, where police work openly with members of specific communities or organizations to facilitate a neighborhood watch; and (3) confidential informants who discretely provide police with detailed information on targeted terrorist groups and their support base.

1. Public Awareness Campaign

Law enforcement officers often cannot observe terrorist indicators directly, while human source networks provide the necessary coverage. An informed, alert community becomes a force multiplier for the police, with countless eyes and ears keeping a lookout.

National Sheriff's Association member Dean Keuter, Jr., founded the Neighborhood Watch program in 1972 with the goal of energizing citizens to spot and report criminal activity in their residential areas. President Bush's administration

established the USA Freedom Corps following 9/11 to curb terrorism in the United States, and one of the Corps' subordinate organs, the Citizen Corps, subsumed the Neighborhood Watch program. The government soon allocated funding to bolster and expand Neighborhood Watch, with a new aim to detect and report terrorist-related activity.[108]

Public awareness (PA) *campaigns* provide authorities a potential network of eyes and ears that can detect indicators of terrorist presence and activity. Such a program's success hinges on active involvement on the part of the citizens and the police. Merely advertising a hotline and encouraging the public to report "suspicious activity" will prove insufficient and potentially problematic. The authorities must educate the public for the initiative to succeed; without proper training or education on what constitutes "suspicious activity," the citizens may fall into the trap of reporting on what they perceive as *suspicious people*, often people who just happen to be different from them—usually ethnically different. The result—heightened ethnic tensions in the community—can prove counterproductive, both by eliciting false positives and by alienating segments of the population.[109]

Citizens can recognize uncharacteristic behavior and occurrences in their neighborhood, but sometimes terrorist indicators are subtle, and people don't always see the connection between something odd and something potentially sinister. The PA campaign must advise people what specific things should concern them, and what types of observations they should report. The U.S. Air Force Eagle Eyes campaign represents a good benchmark. The Air Force reached out to the communities near Air Force installations in an effort to build neighborhood observation networks outside the base perimeters.[110] The campaign included radio, television and billboard advertisements;

[108] Ted Gottfried, *Homeland Security Versus Constitutional Rights* (Brookfield, CT: Twenty-First Century Books, 2003), p. 67

[109] Ibid., pp. 70-74.

[110] Drawn from author's operational field experience.

pamphlets and briefings; as well as door-to-door appeals in the neighboring communities[111] by base law enforcement officials.

An active public awareness campaign sets the antiterrorism agenda in the community and invites people to take information to the police. The next level removes the police from behind the hotline telephone and into the streets, putting them into close working contact with the community citizens.

2. Open Contacts

Law enforcement agencies can maintain regular *open contacts* in the community. These people serve as regular sources of information, the nature of which exposes them to very little personal risk. Thus, the police do not need to handle them as confidential informants or protect their identity. Open contacts have access to information which police may find useful, but they are not levied to undertake operational activity, such as seek contact with terrorist suspects or actively pursue information directly from suspects. Their association with the authorities may be acknowledged, or at least not disavowed if kept somewhat quiet.

An open contact normally maintains a position or location to see occasional terrorist activity indicators, or may be well placed to see them routinely. Should the open contact find himself routinely reporting, where contact with suspect individuals appears likely, the handlers should consider converting the open contact into a confidential informant in the interest of source safety and operational security.

3. Confidential Informants

Confidential informants potentially provide the most detailed and specific information police can hope to acquire about terrorist suspects. Their proximity and access to potential terrorists and their associates gives them unique insight, but also places them at greater risk. If the suspects discover an informant's association with the authorities, both the collection operation and the informant become compromised. The loss to the operation may be months or years of investigative effort. The loss to the

[111] Cliff Mariani strongly encourages personal contact and appeals in establishing a neighborhood "Eyes and Ears" initiative. See Cliff Mariani, *Terrorism Prevention and Response: The Definitive Law Enforcement Guide to Prepare for Terrorist Activity*, 2nd Edition (New York, NY: Looseleaf Law Publications, Inc., 2004), pp. 126-128, 132-133.

informant may be even greater. Therefore, a confidential informant's identity, and his relationship with the police, must remain secret.

E. SOURCE ACCESS

One may categorize the various human sources of information, be they neighborhood watchers, open contacts or recruited informants, by the type of access they have to terrorist-related information.

1. Unassociated Observers

Those sources who have no expected contact or association with terrorists may still be in a position to observe emergent terrorist activity. Such *unassociated observers* would include people who live or work in a location from which they may observe pre-operational terrorist preparation, such as target surveillance or supply acquisition. One will generally find these sources around potential terrorist targets, or places where terrorists might acquire operational materials. A retired woman[112] who lives across the street from a potential terrorist target may be in a position to see such surveillance. A transit authority employee, like a token booth clerk or facility custodian, might similarly be positioned to recognize pre-operational reconnaissance of a subway station, or even an attack rehearsal. A wholesale farming supply store clerk can identify bulk fertilizer purchases by customers who don't quite resemble farmers or landscapers. The specific odds are small that any single individual will witness terrorist indicators, but enlisting them as lookouts and educating them on what to look for expands the overall information input. Unassociated observers may come forward in response to the public awareness campaign, or the police might recruit them individually as open contacts.

2. Proximal Outsiders

Proximal outsiders are people tangentially affiliated with suspected terrorists, or who are in close proximity to them. Fellow mosque congregants, neighbors, school classmates, co-workers or employers may all be able to observe the suspects' behavior and report it to authorities. Unlike unassociated observers, proximal outsiders are not necessarily placed near targets or material resources. Rather, they enjoy placement near

[112] Retired people and senior citizens can make good lookouts because many spend much of their time at home, giving them nearly continuous coverage of their field of observation, and because "they are likely to be mature, focused and dedicated to their [task]." See Mariani, p. 132.

the terrorist suspects themselves. Police can handle such sources as either open contacts or confidential informants, depending on the level of risk involved with their reporting.

3. Detached Associates

Terrorists cannot operate in a vacuum. They require some measure of life support from their community, even from those people who may not support their violent agenda. Terrorists depend on direct and routine support from clerics, grocers or landlords to get along in daily life. These *detached associates* enjoy ongoing access to the suspects, and if they do not endorse a terrorist cause, may prove to be willing recruits for police. They normally will act as open contacts or confidential informants, again depending upon the frequency and intimacy of their contact with the suspects and the attendant risk they face in reporting to police.

4. Network Members

An inside member of a terrorist organization is the Holy Grail of source recruitment. Network members have a direct stake in the terrorist agenda as participants of some kind. They may be actual terrorist operatives, such as bomb technicians, target scouts or attackers. Or, they may directly support operatives as safe house proprietors, couriers, propagandists, trainers, radical imams or doctors who privately treat injured operatives. Police who successfully turn a network member as a recruited source (commonly called a "flipped" source) enjoy very detailed operational information about the group—assuming the source is faithfully working for the police and not acting as a double agent. Police should always handle a flipped source as a confidential informant, as the risks to the source and the police investigation are extreme.

F. SOURCE PLACEMENT

A source's access to information normally derives from the source's *placement* with respect to terrorists or their activities. Placement determines the type of sourcing operation his handlers will employ him for.

One will generally find unassociated observers near a specific resource terrorists might need to acquire for operations, or near a potential asset the terrorists might target for an attack. An unassociated observer may never see a terrorist. However, the source serves as a watchman or a human alarm, poised to alert authorities in the event a suspected terrorist enters his area of observation.

Proximal outsiders may enjoy either resource-specific or suspect-specific placement. Authorities recruit sources with resource-specific placement to report any indicators of emergent terrorist activity or presence. Unlike unassociated observers, proximal outsiders—like mosque congregants or neighborhood residents—are positioned in places terrorists can be expected to emerge and establish a continuous presence, or even a base of operations. Police may also levy proximal outsiders to observe specific people, in which case they enjoy suspect-specific placement. Investigators may gather information on a suspected terrorist by directing his fellow congregants, neighbors, co-workers or classmates to report on his activities.

Detached associates may also have either resource-specific or suspect-specific access. An imam, *halal*[113] grocer, or employee at the university Islamic center are in a good position to identify any emergent radical elements in their midst, constituting resource-specific access. (That is, they are positioned at a resource of which Islamist terrorists may routinely partake, be it religious services, Islamically appropriate foodstuffs or community fellowship.) Police can brainstorm about what employment a terrorist scout might seek in order to gain access to potential targets, and then recruit sources within that job field. For example, they may recruit a foreman at a construction firm doing maintenance on a high-profile landmark identified as an attractive target for terrorists. The foreman can then report on any employees, or prospective employees, who appear more interested in details about the potential target than their assigned tasks. Thus, employers and potential employers represent good sources. Additionally, police may levy these same sources to keep an eye on any suspect individuals previously identified. The sources would, in such circumstances, have suspect-specific access.

Recruited network members offer police direct insight into a terrorist organization and its members. Therefore, their access is suspect-specific.

The process of selecting sources with advantageous placement and access seems straightforward. However, identifying good potential sources, not to mention actually recruiting them, becomes increasingly challenging when police officers must reach out to

[113] *Halal* constitutes Islamic dietary strictures, similar to *Kosher* in Judaism.

an ethnic, immigrant community to find them. Operating in an environment shrouded in a foreign culture requires savvy and subtlety.

G. SOURCING IN AN ETHNIC IMMIGRANT COMMUNITY

1. Reducing Fear, Building Trust

Traditional ethnic, immigrant communities are those whose residents tend to adhere to social and cultural mores from their home of origin, and who have not fully assimilated into the mainstream American culture. These sub-societies tend to be insular. The members may communicate primarily—or exclusively—in their native tongue, and limit their associations outside of the community. Law enforcement officers serving a traditional ethnic, immigrant community must overcome the apparent cultural divide to be effective, particularly when attempting to enlist the community's assistance with crime prevention or antiterrorism programs.

Officers working with an immigrant community must understand the culture as well as possible. Understanding the customs, fears and cultural taboos will help the officers interact properly with the neighborhood residents and sidestep potential misunderstandings or friction. A woman immigrant from the Middle East may resist speaking with a male police officer, deferring to her husband; another may speak with the officer, but refuse to make eye contact. An officer untrained in the cultural mores might read such behavior as deceptive, which might induce him to regard the woman with suspicion, or even list her mistakenly as a criminal suspect.

When members of the police department recognize a community's cultural nuances, the department can better plan its engagement. Immigrants hailing from oppressive Middle Eastern regimes often regard plainclothed detectives with suspicion or fear, because plain clothes in the old country were the hallmark of the secret police, not detectives or criminal investigators. Secret police represent the government's heavy hand; they protect and serve the regime's stability, not the citizenry. Departments dealing with a traditional Arab immigrant enclave might do well to dispatch uniformed patrol officers to the neighborhood, rather than plainclothed detectives or agents.[114]

[114] First Technologies, LLC., 16-17 September 2004.

Sometimes Middle Eastern or Middle Asian men will refuse to deal with a female law enforcement officer, or will do so grudgingly, which might induce a department to exclude women officers from handling the neighborhood. This shortsighted approach blinds the department to half the information available in the community. When a man refuses to work with women officers, odds are the wife and the other women in his household will be reluctant to speak openly with male officers. If they do speak with a male officer, the man of the house might insist on being present. This naturally stifles any frank testimony on the women's part, especially in incidents like domestic abuse. A woman officer, however, may find inroads into the female population, not only uncovering criminal activity, but possibly identifying points of inquiry regarding terrorism or Islamic extremism. For example, the patrol officers with a metropolitan police department had just undergone Middle Eastern cultural awareness training the day before.[115] One patrol was dispatched to a domestic disturbance in a Middle Eastern household. When the patrol officers arrived, they took a statement from the husband, but sensed the wife was withholding on her testimony. They recognized the cultural issues at play, based on the previous day's training, so they sent a female patrol officer the next day to speak with the wife while her husband was away at work. The wife explained she and her husband had fought because he had fallen in with some bad elements at the mosque, and she was concerned he might jeopardize the life they had worked so hard to build in America. This tidbit constituted a lead the police could further pursue to identify some potential radical Islamists.

Law enforcement officials get "paid to be paranoid," and they necessarily approach many aspects of investigative work with circumspection. Nevertheless, officers must learn to disguise their suspicions and apprehensions to interact effectively with witnesses and suspects alike. (Sometimes a detective does not want a criminal suspect to catch on too soon that he is under suspicion, lest it derail the investigation.) Police should take a similar tack when they approach immigrant or minority communities, where the members may already feel uncomfortable with outside authority figures or the

[115] Special Agent Ariel Benjamin Mannes, Transportation Security Administration, Department of Homeland Security, "Interagency Intelligence Sharing and Analysis: Resources in the Homeland Security Reporting Process," International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL, lecture, 20 October 2005. The specific city and department have been masked for security purposes.

larger American society. This becomes especially important when pursuing criminal or terrorist elements who identify with a narrow ethnic or religious segment in society, because the radius of inquiry focuses on that small segment. If the community feels threatened, it may circle the wagons and refuse to cooperate with the police, or at best do so reluctantly. Not surprisingly, the carrot often yields better results than the stick.

2. Using the Stick

The FBI's approach to mass interviews of Arab-Americans and Muslim Americans in November 2001 portrayed an overarching sense of suspicion. Many interviewees complained they felt the interviews were more akin to interrogations, and they felt the FBI agents treated them more as suspects than potential witnesses. This alienated an important population segment that the country needed for its antiterrorism efforts.[116] One can imagine the difficulties the FBI encountered later when it tried to recruit Arabic linguists into government service.

Officers must carefully plan their interaction, bearing in mind cultural sensitivities and language barriers, to avoid alienating potential witnesses or sources of information. They can appeal to civic-minded members of the community to help identify criminal or terrorist elements in their midst—something that will benefit both the police and the community.

3. Using the Carrot[117]

The members of a local Muslim congregation fell under intense scrutiny immediately following 11 September. The outside community cast tremendous suspicion on them, and local authorities repeatedly approached the imam and demanded he identify any terrorists in his mosque. The local police stationed patrol units on surveillance detail outside the mosque complex (including its community center and living quarters), essentially placing the community under quasi-house arrest.

---

[116] For a critique on post-9/11 U.S. Government policies that apparently singled out Arabs and Muslims in America, see Louise Cainkar, "Post 9/11 Domestic Policies Affecting U.S. Arabs and Muslims: A Brief Review," *Comparative Studies of South Asia, Africa and the Middle East*, 24:1 (2004): 245-248, http://muse.jhu.edu/demo/comparative_studies_of_south_asia_africa_and_the_middle_east/v024/24.1cainkar02.pdf (accessed 29 November 2005).

[117] Drawn from the author's discussions with the parties involved during his professional field experience. The specific agency and location have been omitted for security purposes.

The special agent-in-charge of a nearby federal investigative office sent an envoy of agents to the mosque, with specific instructions on how to approach the imam. The agents arrived and told the imam they understood his congregants were catching a lot of unwarranted grief, and they asked him, "How are *you* guys holding up? Is there anything we can do to help you?" The imam replied that they were the first people to show any concern for his community, and the first to offer any assistance. Up until that point, the local authorities approached the mosque with the apparent presumption the community was harboring terrorists. In reality, the imam was more than eager to root out any bad apples in his midst, as they would only make life more difficult for his congregation. The agents partnered with the imam on the spot, who used his extensive contacts through the greater Muslim community to identify any potential radicalism or terrorist leanings.

4. Finding the Focal Point

Looking for sources can resemble prospecting for oil. One can randomly drill, hoping to stumble upon a decent source. Conversely, one can do a little research, find the right spot, and strike a gusher. The imam at a local mosque can be a valuable ally in an antiterrorism campaign. He can identify suspect newcomers who appear to espouse radical or violent views, or point out Salafist cliques. The imam may also tell authorities about radical visiting clerics on speaking circuits, or suggest which other mosques and imams in the area have radical inclinations.

Police may find other potential sources in the neighborhood outside of the mosque itself. Traditional immigrant communities often import their social structure from the home region, crafting a neighborhood hierarchy that functions like a community government. Traditional Middle Eastern immigrant neighborhoods usually model themselves like a village back home, with one clear leader. The *mukhtar* ("the elected one")[118] serves as the village elder, working to maintain order in the neighborhood. He helps resolve disputes, gets newcomers settled in, and may also monitor or guide the neighborhood's interaction with the outside society. Culture and language barriers heighten the importance of the *mukhtar*'s liaison function, since many immigrants need assistance setting up utilities, filing taxes, or getting a driver's license.

[118] Joseph Odisho, U.S. Government contract linguist, personal conversation during USAF Special Investigations Academy Critical Threat Counterintelligence Collections Course, 2005.

The *mukhtar* is normally an older male who has been in country for a number of years. Strongly wired into his community, he knows all of the residents and knows more than anyone else what occurs in the neighborhood. Thus, he represents the greatest potential source for police. The *mukhtar*, if recruited, can be an invaluable resource. How can one identify the *mukhtar*? Generally, he's the first person anyone in the neighborhood calls in a crisis. He's the one they call *before* they dial 911. And he is the man already on scene when the first responders arrive,[119] either quietly observing or actively ensuring his constituents are properly cared for. Antiterrorism investigators can train first responders, like patrol officers, firefighters and emergency medical technicians, on what to look for and how to identify the *mukhtar*. Additionally, the first responders can ask the *mukhtar* for his contact information, which they can pass to the investigators so they may introduce themselves at a later time. Alternatively, if a department has a branch of antiterrorism specialists, they may take rotations on call, responding to any 911 call in a neighborhood of interest, so they may personally meet the *mukhtar* on scene and introduce themselves.

A sourcing focal point, like an imam or *mukhtar*, will generally act as a source handler himself, essentially managing neighborhood residents as sub-sources, and then passing the information to the police. Sometimes, however, he may introduce police officers to trusted members of the community, who in turn can become sources (either open contacts or confidential informants). The focal point can help officers integrate with the neighborhood in setting up a community policing or neighborhood watch program. As a trusted leader, the *mukhtar* or imam can personally introduce plainclothed officers to the neighborhood residents, thereby helping to overcome the immigrants' inherent fear and mistrust of police in civilian clothes.

Human intelligence lends itself well to preventive antiterrorism operations, and plays to the strengths of the law enforcement community. Police routinely employ human informants in criminal investigative work. Proper planning and training can help authorities readily adapt the tool to a new operational target and objective, giving them an edge in combating terrorism in their respective jurisdictions.

[119] First Technologies, LLC., 16-17 September 2004.

IV. ANTITERRORISM ANALYSIS FOR THE LAW ENFORCEMENT COMMUNITY: PUTTING THE PIECES TOGETHER

Surprise attacks succeed when intelligence analysis fails. From Pearl Harbor to 11 September, post mortem investigations disclose that various people have clues pointing to an upcoming event, but nobody gathers all of the clues and assesses them to predict an attack. Solid intelligence analysis underpins any effective antiterrorism program. The goals of analysis are to learn about current terrorist methods and to predict their future actions—and thereby prevent an attack. Understanding the terrorist methodology gives analysts insight into what steps terrorists must take in order to execute an attack, and those steps exhibit observable signatures, or indicators. When field collectors recognize and report those indicators, the analysts can piece together a prediction of an impending terrorist operation.

Analysts must be aware of certain tendencies in the human thought process—assumptions and mental shortcuts—that can lead them to erroneous judgments. They must also contend with another potential stumbling block: the tremendous volume of raw data they must comb through to extract relevant details and develop terrorist behavior patterns. Fortunately, automated analytical systems can help. They are not a stand-alone tool, however, as human analysts must interpret the computer's findings.

The global jihad's dispersed nature imposes certain structural requirements on antiterrorism analysis that span from local to national-level efforts. Al-Qaeda and the other participants in the global jihad have demonstrated the ability to run operations against similar targets in different localities (or even different countries). This phenomenon may be the result of operational design, as in al-Qa'eda's simultaneous attacks on separate targets, or simply the result of imitation and collaboration between geographically separated, semi-autonomous cells. In either case, jihadi activities may exhibit patterns that are only evident at a regional or national level. Law enforcement analysts in a local jurisdiction cannot see the larger patterns of terrorist activity across a wider geographic area; observers at a regional or national level are better suited to recognize a dispersed pattern. Conversely, analysts at higher echelons have no visibility

of localized events unless the local jurisdictions pass the information up to them. Finally, local departments often lack the resources and training to field an effective analytical capability, thus placing a heavier load on regional and national analysts.[120] Properly structuring law enforcement analytic units can help tie local, regional and national assets and information together to form an effective antiterrorism intelligence cooperative.

A. A LOST ART

Police departments and law enforcement agencies across the nation are striving to gather information about threats, with emphasis on training officers about pre-operational indicators and clues of terrorist activity, and with a strong push toward recruiting informants. Intelligence collection constitutes the first step in the proactive terrorism counteraction chain, but all that information adds little value if it isn't analyzed to ascertain its significance and put it into a larger context. Intelligence analysis makes collected information useful and gives it meaning. The analyzed intelligence (called *finished intelligence*) ultimately informs a battery of intelligence consumers—policy makers, resource owners, enforcement officers and field collectors alike. Analysis, employed properly, helps craft suitable defensive measures to meet the terrorist threat, assists investigators to develop investigative plans, enables enforcement and disruption operations, and provides structure to ongoing intelligence collections. Consequently, for any organization confronting terrorism, including law enforcement, a properly formulated terrorism counteraction program necessitates a solid, structured analytic underpinning. Unfortunately, police departments and larger law enforcement organizations alike usually lack the resources to recruit and properly train analysts in the science—and art—of intelligence assessment; even the national Intelligence Community faces these challenges. Furthermore, the analytical process often stands far removed from the action in the field or on the street, so it remains under-appreciated, misunderstood and often neglected…until something goes wrong.

B. INTELLIGENCE FAILURES: EYE ON ANALYSIS

Pundits liken 9/11 to Pearl Harbor. Both represent watershed events for America's Intelligence Community; both have been labeled catastrophic "intelligence failures." The Pearl Harbor attack ultimately precipitated the National Security Act of

[120] Brian Michael Jenkins, *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves* (Santa Monica, CA: RAND, 2006), pp. 164-167.

1947, which established the Central Intelligence Agency (CIA) and the US Intelligence Community, all elements of which were subordinated to the Director of Central Intelligence (DCI). All intelligence agencies were supposed to follow the DCI's direction to ensure a national unity of effort in intelligence matters, and all collected national-level intelligence thenceforth flowed through the CIA to ensure it could be centrally analyzed to prevent another surprise attack. Nearly sixty years later, America had its second Pearl Harbor, and the 9/11 Commission subsequently recommended assigning a national intelligence director over the Intelligence Community to ensure unity of effort and centralized analysis.[121] (The only difference between the DCI as established by the National Security Act of 1947, and the new director proposed by the Commission—now called the Director of National Intelligence, or DNI—is the titular head of the Intelligence Community would be divorced from the CIA. The National Security Act previously charged the DCI with dual responsibilities as the head of the CIA and the leader of the overall Intelligence Community.)

Just what was the "intelligence failure" in each case? Some people might suggest the Intelligence Community did not have enough information to forecast the attacks. This is not necessarily so. The 9/11 failure mirrors past intelligence shortcomings in which the U.S. has been caught off-guard by adversaries. Michael Handel contends that "past failures in avoiding surprise cannot be blamed on a dearth of information and warning signs. Consequently, one must look to the levels of analysis and [policymaker] acceptance [of intelligence] for an answer."[122] There were indications of impending Japanese hostilities prior to the attack on Pearl Harbor, but the U.S. intelligence elements lacked the necessary coordination or analysis to recognize them.[123] The Federal Bureau of Investigation had specific information before September 2001 concerning Arabs, possibly linked to Osama bin Laden, taking pilot lessons in the U.S.; the absence of

---

[121] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, authorized edition [paperback] (New York, NY: W.W. Norton & Company, Inc., [2004]) pp. 399-400, 411-415.

[122] Michael I. Handel, "Intelligence and the Problem of Strategic Surprise," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, eds. Richard K. Betts and Thomas G. Mahnken (Portland, OR: Frank Cass Publishers, 2003), p. 8.

[123] Abram N. Shulsky and Gary J. Schmitt, *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. (Washington, DC: Brassey's, Inc., 2002), p. 161.

timely distribution and centralized evaluation of these disparate reports made headlines after the "Phoenix Memo" became public.[124] Raw information was available in both cases. U.S. Air Force intelligence analyst Sundri Khalsa asserts, "Warning failures are rarely due to inadequate collection [and] are more frequently due to weak analysis."[125] The raw information was not properly centrally analyzed to develop patterns and trends that might suggest impending attacks. The Intelligence Community—and the law enforcement community—lacked sufficient predictive analysis to yield a warning. Above all else, threat warning represents the most visible and salient goal of intelligence analysis.

C. BROAD GOALS OF TERRORISM ANALYSIS

Mark Kauppi, a program manager for the Counterterrorism Training Program at the Defense Intelligence Agency, says that terrorism intelligence analysis "aims to improve our understanding of terrorist activities (what they do), their motivation (why they do what they do) and organizational associations (how they are organized to carry out their activities)."[126] The desired end result is a greater awareness of the terrorist threats, the disruption or neutralization of terrorist activities and organizations, and advanced forecasting and warning of impending attacks.[127] Kauppi insists this last service, the warning of attacks, is the analyst's "number one job." Analysis yields "three levels of warning. Most important is tactical level warning," which is time-sensitive (usually within hours or days) and target-target specific, sometimes with details about the method of attack. Operational level warning is less specific regarding location (perhaps only narrowed down to a geographic region) or attack details and covers a time window of weeks or months. Strategic warning is very general and covers a timeframe from several months to several years.[128]

---

[124] *The 9/11 Commission Report*, pp. 83, 272, 347, 497.

[125] Captain Sundri K. Khalsa, USAF, "Terrorism Forecasting: A Web-Based Methodology," *Occasional Paper Number Eleven* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004), p. 21.

[126] Mark V. Kauppi, "Counterterrorism Analysis 101," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 39.

[127] Ibid., pp. 39-40.

[128] Ibid., p. 40.

Precisely what is this mystical process called "intelligence analysis"? *Webster's* dictionary defines it as the "separation of a whole into its component parts," or "an examination of a complex, its elements, and their relations."[129] Analysis is at times the process of breaking down collected information for examination, and alternately assembling the various pieces "into something that is usable by" a given consumer.[130] An analyst must often deal with uncertainty introduced by incomplete or imperfect information. Therefore, judgment becomes a crucial component of his intelligence assessments,[131] whereby he weighs evidence (collected data) and forms estimates of what he believes represents reality. The pictures the analyst paints include descriptions of present reality and predictions of potential future events. Each class of analytical product serves different purposes.

D. ILLUSTRATING THE PRESENT

A terrorism analyst first educates his customers by framing the world in an understandable fashion. He takes pieces of collected information and crafts a picture—often a "best guess" picture founded on incomplete information—that describes or explains terrorist phenomena and threats. Case studies on terrorist groups and incidents provide insight into their methods, resources, personnel and capabilities. Their documents and rhetoric further elucidate their methods, intentions and mindset.

Viewing the intelligence picture over time, an analyst hopes to identify patterns—hallmarks that consistently manifest themselves whenever a certain process or series of events occurs. Kauppi explains, "A pattern is simply repeated behavior over time."[132] Patterns often derive from examining a broad sweep of field reports and previous, relevant analytical products; the analyst seeks out repetition in the details. Once an analyst identifies a pattern, changes in that pattern become easier to recognize. Such a "change in the pattern of behavior" is called a trend.[133] "[Identifying] a group's pattern

---

[129] *Webster's Ninth New Collegiate Dictionary* (Springfield, MA: Merriam-Webster, Inc., 1987), p. 82.

[130] Shulsky and Schmitt, p. 41.

[131] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence [Central Intelligence Agency], 1999), pp. 31-32.

[132] Kauppi, p. 47.

[133] Ibid., p. 47.

of behavior is imperative in order to establish a baseline of how terrorists go about doing what they do…the traditional modus operandi or pattern of terrorist activities…."[134]

The analyst can dissect case studies, training documents and doctrinal materials to piece together a particular group's *modus operandi*. He can formulate the MO into a model his customers—patrolmen, investigators, security professionals and policy makers—can use to inform their operations and decisions.

Outlining a terrorist group's MO, the analyst helps investigators plan their investigations and operations by giving them insight into their target (the terrorist group), and more specifically, potential vulnerabilities in the terrorist planning and attack cycle.[135] The MO can also point them toward potential sources of information or investigative leads to pursue.

A detailed MO also informs policy makers and those responsible for securing public or private sector resources. The resource security managers, once knowledgeable of the possible methods of attack, can devise defensive plans and countermeasures, weighing the risks against the defensive measures' potential costs.[136] The risk assessment depends significantly on the analyst's threat picture, that is, the evaluation of the threat posed by terrorists: their preferred attack methods and attendant capabilities (their MO), their goals and intentions, plus an estimate of the likelihood that they will attack a specific target or set of targets.[137] Herein the analyst parlays the current intelligence picture into a prediction of possible future terrorist events.

E. PREDICTING THE FUTURE

Crystal balls are in short supply, and they don't work very well anyway, so an analyst must seize other means to peek into the future. Forecasting terrorist events arguably overshadows all other analytical functions, since the failure to anticipate an attack carries grave consequences. Threat warning is a product of indications and

---

[134] Kauppi., p. 48.

[135] For a brief description of the attack cycle, see "Vulnerabilities in the Terrorist Attack Cycle," *STRATFOR* (Strategic Forecasting, Inc.), 29 September 2005, http://www.stratfor.com/products/premium/print.php?storyId=256319 (accessed 6 March 2006).

[136] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York, NY: Copernicus Books, 2003), pp. 14-15.

[137] Ibid., pp. 78-79.

warning, or I&W, intelligence. I&W derives from tactical collection of discrete indicators combined with trend analysis. The process points to future developments and puts the incoming indicator data into context.

An indicator is some piece of information (normally an observable event) that points to a step in a process.[138] An indicator resembles a box in a checklist; once an event is observed that corresponds to an indicator, it is called an indication.[139] Khalsa notes, "Indications are activities that *have happened* that fall into one of the indicator categories" (emphasis hers).[140] Indicators help analysts "diagnose a decision, condition, or process"[141] which a terrorist entity undertakes. For indicators to be useful, they must represent behavior or events that manifest themselves predictably and repeatedly any time a given process occurs.[142] In other words, they must show fidelity to an established pattern an analyst has previously discerned about terrorist activity. Likewise, indicators must be observable to serve their function; if a terrorist process includes a secret step that field collectors will never see, it has no value as an indicator.[143] It's a box on the checklist that will never be marked.

The analyst interpolates indicators from a model of a terrorist process (e.g., a given group's preferred attack method). They can deduce indicators from:

- Steps the terrorists must take to complete the process;
- Previous incidents and behavior attributed to the group;
- Actions that cannot be circumvented, such as crossing a border or approaching the target;
- Terrorist group rhetoric, statements or doctrine;
- Training programs or training materials;

---

[138] Shulsky and Schmitt, p. 59.

[139] Ibid., p. 59.

[140] Khalsa, p. 13.

[141] McCreary, John F., Defense Intelligence Agency, Presentation on Indications and Warning Analysis, lecture with handouts, Naval Postgraduate School, Monterey, CA, 22 February, 2006).

[142] Ibid.

[143] Ibid.

- People with knowledge about the process, such as inside informants or observers.[144]

The indicators, listed as a sequence of discrete, consecutive events, effectively establish a timeline for the analyst.[145] As the analyst annotates the occurrence of indications (events that have happened and have been observed), he can establish how far along the chain of events a terrorist group has progressed, and what future events, represented by indicators, one can expect to be forthcoming. This forecasting constitutes the warning portion of the I&W process. The following example depicts a hypothetical indicator sequence.

F. TERRORIST ATTACK PROCESS INDICATOR SEQUENCE

The Al-Qa'eda attack process (derived from the *Military Studies in the Jihad against the Tyrants*)[146] follows:

1) Research and reconnaissance phase
   a) Visual reconnaissance or surveillance of target*
   b) Checking time of certain events (i.e., checking watch)*

2) Planning phase
   a) Draft plans
   b) Discuss plans with team members (team meeting)*
   c) Modify plans as required

3) Execution phase
   a) Pre-deploy attackers and/or weapons to staging area*
   b) Confirmatory target reconnaissance or surveillance*
   c) Deploy attackers and/or weapons to attack site*
   d) Activate weapon (i.e., draw firearm or actuate detonator)*

[144] McCreary.

[145] Ibid.

[146] *Military Studies in the Jihad against the Tyrants* [a.k.a. *The al-Qa'eda Terrorist Training Manual* or *The Encyclopedia of Jihad*], [attributed to Al-Qa'eda, ca. 1992 or 1993, translated by the Greater Manchester Constabulary, UK, ca. 2002], pp. UK/BM-71-73.

The steps marked with asterisks (*) constitute indicators because they represent steps that are collectable, although gaining access to some of them may require penetration of the cell by technical means or an informant.

The indicator chain would look like this:

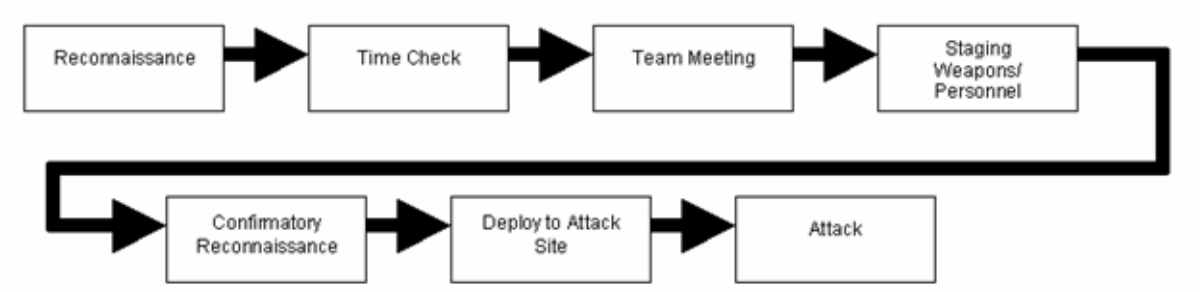

Figure 2 Indicator Chain

A field collector reports hostile surveillance of a power plant. The analyst notes it on the indicator sequence:

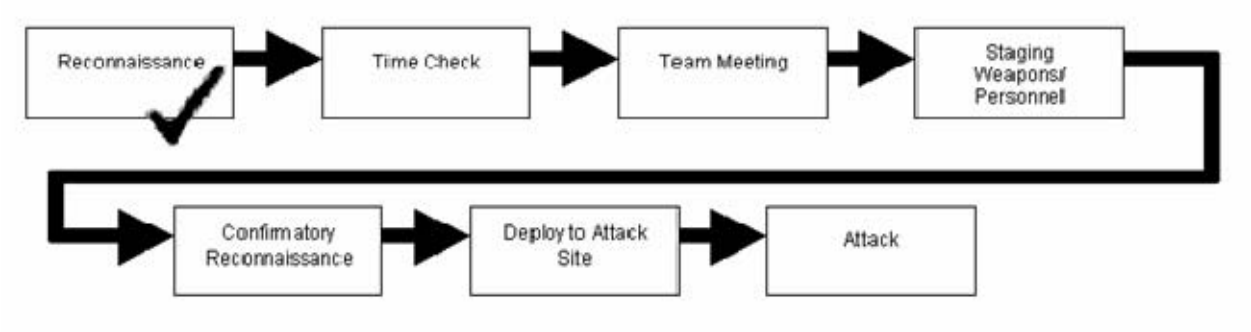

Figure 3 Indicator Chain – Reconnaissance

A subsequent report advises that a hostile surveillant was seen checking his watch when the facility guards conducted shift change. The analyst notes that indicator:

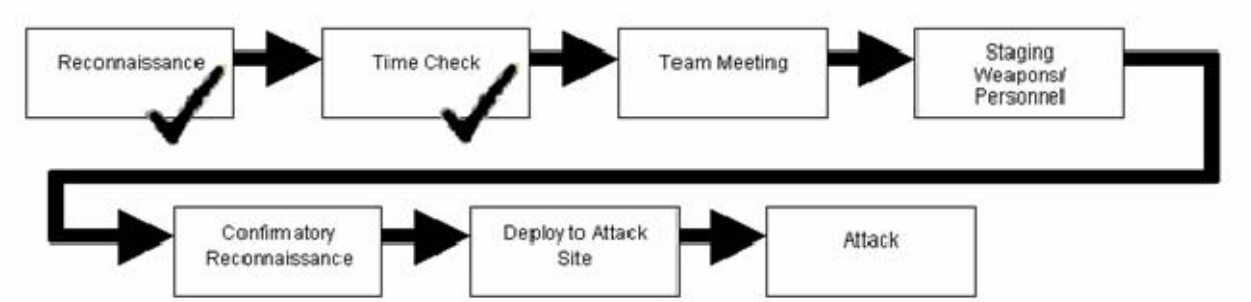

Figure 4 Indicator Chain – Time Check

Yet another report comes in that suggests new people have arrived in the local area, and known Islamists were observed moving crates into a self-storage unit a mile from the power plant. It appears collectors have not been able to gather any information on a possible team meeting, but the sequence of events has become evident to the analyst. He advises the field collectors to stay attuned to a possible re-emergence of reconnaissance or surveillance around the plant. They are now looking for the next indicator in the chain.

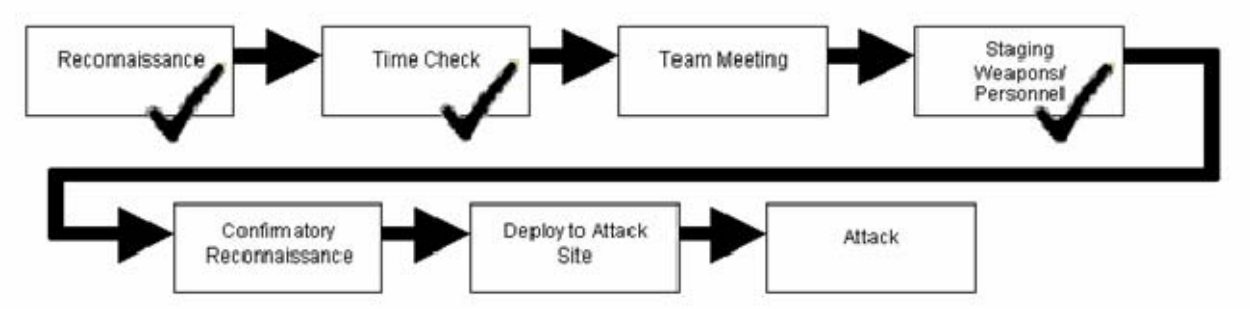

Figure 5 Indicator Chain – Staging

The officers report another round of surveillance. The analyst forecasts an attack in the near future, and recommends heightened security measures.

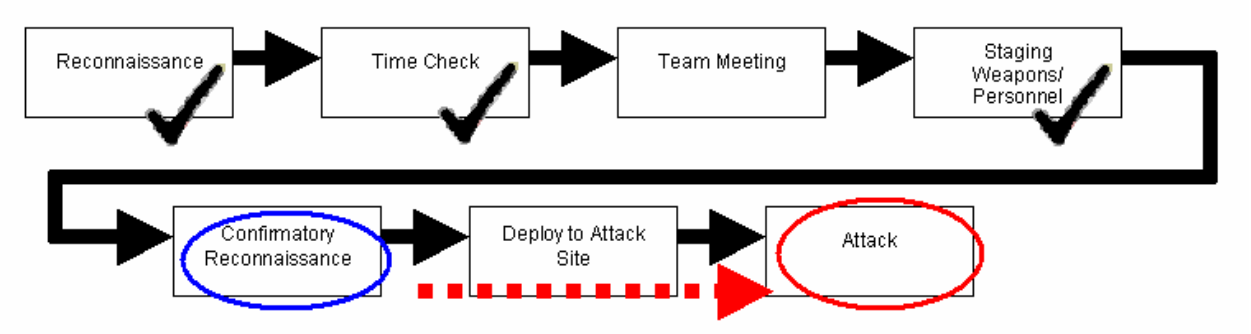

Figure 6 Indicator Chain – Forecast

G. THE ANALYSIS PROCESS

Intelligence production constitutes an iterative process wherein the players interact and coordinate their functions. A good analyst will work with field collectors and guide their collection activities. The analyst should first ascertain what intelligence he needs concerning the terrorist threat picture to support his various consumers. He then assesses what information he has, and what information he lacks (called an *intelligence gap*), in addressing the intelligence needs. The analyst levies the collectors with categories of information they ought to gather, or simply, *collection requirements*. Examples might include "terrorist safe house information," "terrorist weapons and tactics," or "vehicle data." Specific details to acquire, such as names, vehicle models and colors, license plate numbers, telephone numbers or addresses, are called *interrogatories*. Together, these levies constitute an intelligence shopping list for the field collectors. (Patrol officers and investigators represent the law enforcement community's field collectors.)

As the collectors gather information and submit field reports, the analyst provides feedback on the quality and relevance of the intelligence, advises on how to sustain or improve the quality, and suggests where to focus future collection efforts.[147] The intelligence consumers, likewise, should reciprocate with feedback on the value of the finished (i.e., analyzed) intelligence the analyst produces.

This resembles a simplified version of the national Intelligence Community's intelligence cycle.[148] The intelligence consumers—government officials or other

[147] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, DC: CQ Press, 2006), p. 64.

[148] Ibid., p. 65.

decision makers who rely on intelligence to formulate policy and strategy—ideally work in the planning and direction phase, advising the intelligence elements what kind of intelligence they want produced. Field collectors gather information during the collection phase and, in the processing phase, translate (or collate) it into a format the analyst can readily use, normally a field report. The analyst receives and assesses the field reports, churning out finished analytical products in the analysis and production phase. He provides feedback to the collectors about the quality of the information they've gathered, as described above. The analyst then delivers the finished intelligence assessments to the consumers in the dissemination phase. Again, feedback comes into play, only this time it's from the consumers, evaluating the quality of the finished intelligence the analyst produced. Then the cycle begins anew, with the consumers re-examining what intelligence they have and what intelligence they still need to support their decisions. Figure 7 depicts the intelligence cycle.

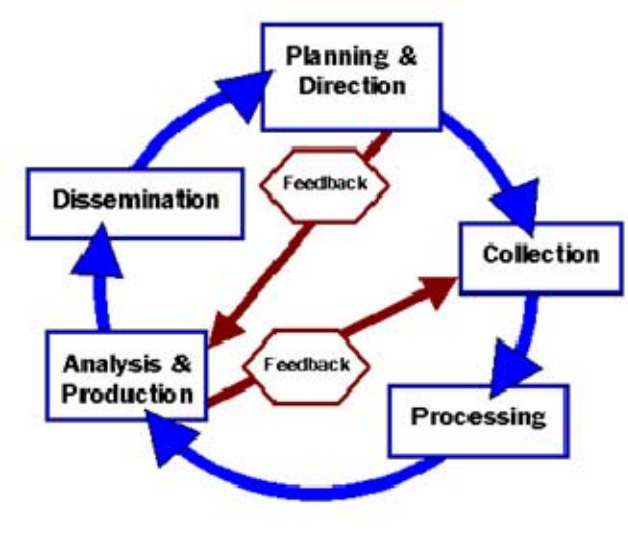

Figure 7 The Intelligence Cycle

Law enforcement intelligence operations, especially at state level and below, will generally find the intelligence actors sharing roles, and fulfilling multiple roles, across the cycle's various phases. Local consumers of law enforcement intelligence will normally demand more direct analyst involvement in the planning and direction phase to help them determine their intelligence needs, and to articulate them as sensible collection requirements and interrogatories for the field collectors. Day-to-day consumers will not

be limited to public officials, but will include community business owners, industrial security managers, patrol officers and police investigators. Meanwhile, police officers, as field collectors, need analytical products to plan further collections; in their enforcement role, they'll use them to plan investigations and operations, such as raids or arrests. Thus, they are both collectors and consumers.

H. THE SCIENCE OF ANALYSIS

Finished intelligence reports are not mere compilations of raw field data. The analyst imbues the information with meaning and context by fitting it into a construct that explains a given phenomenon, like al-Qa'eda's operational workings. Such insights traditionally derive from an historical evaluation of terrorist groups and their behavior. The construct is a mental model the analyst uses to examine and evaluate a terrorist group or process; it is how he perceives the terrorists and their behavior as drawn from the patterns he has devised from his research. The mental model frames how the analyst evaluates future field reports on the terrorist enterprise. The model itself may be either explicit or implicit, depending on which approach the analyst employs.[149]

The first is the cognitive analytical approach. In this case, the mental model is implicit, not explicit. The analyst may have to construct a model from scratch if evaluating a new phenomenon (a new group, new MO, etc.). This approach is more intuitive and qualitative.[150]

The second is the data-driven analytical approach, which uses an explicit, previously defined model into which incoming data are introduced to generate a conclusion.[151] Indications and warning analysis, with its checklist and fill-in-the-blank methodology, follows a data-driven approach.

One must exercise caution with mental models. A model remains subject to change, either because new intelligence becomes available that contradicts it, or because real conditions change and render the model obsolete. The global jihad continues to evolve and al-Qa'eda's operations tomorrow will probably differ from its operations of yesterday. One need only look to Iraq, the new jihadi training ground, to see how quickly

[149] Heuer, pp. 55-57, 58-60.

[150] Ibid., pp. 59-60.

[151] Ibid., pp. 60-61.

the insurgents adapt their tactics to challenge the Coalition forces. An analyst must accept that his mental model will be a temporary construct, and he must be vigilant for signs of its decreasing validity. He cannot stay wedded to an older model once it becomes obsolete. Unfortunately, humans are loath to change their perception of how the world works; even analysts resist change.[152] Stubborn adherence to a given mental model may constitute a bias, a preconceived outlook that bears directly on an analyst's effectiveness.

An analyst will confront many types of bias, but four warrant special mention. All interact closely when the analyst tackles terrorism, potentially skewing his analytic judgments. The first bias induces analysts to seek out cause-and-effect relationships between observed events.[153] An analyst faced with coincidental and unconnected events might misconstrue a causative relationship, recommending ineffective solutions. The same can be said for related events with a common cause, but have no causative relationship between themselves. In a medical example, doctors used to believe inflamed tonsils caused severely sore throats, and removed the tonsils as the presumed cure. The tonsils, in fact, swell as a result of the infection which simultaneously causes a sore throat; tonsils actually serve as defense organs that protect against infection. The cases in which they become inflamed are instances where the infection overwhelms the tonsils' defenses. The doctors of yesteryear mistakenly attributed a cause-and-effect relationship between two concurrent phenomena.

The analyst is secondly inclined to presume a given group's actions or behaviors are intentional outcomes of centralized planning.[154] If a terrorist operative boards a bus with an explosive satchel and the device detonates, killing the terrorist and the other passengers, an analyst is strongly inclined to presume the operative (1) specifically targeted that bus (2) on orders from his group's leaders, and (3) that he intended to execute a suicide attack. The terrorist, in reality, might have simply received orders to attack any target of his choice, elected to leave a time-bomb at the airport, and was

[152] Heuer, pp. 10-11, 61.

[153] Ibid., pp. 129-131.

[154] Ibid., pp. 131-132.

simply riding the bus to his target when the satchel prematurely exploded. Consequently, it would be specious for the analyst to conclude the terrorist group is targeting commuter buses with suicide bombers.

A centrally controlled, hierarchical model is alluring because it characterizes the group as a single, unitary—and presumably rational[155]—actor that has a single command element (the "brain"). Such an organization is easier to defeat, contain or control than an amorphous, decentralized collective, making it a more palatable adversary; conceptually, this model "is convenient and reassuring"[156] for the analyst and policy maker alike.[157] One can study and anticipate a logical adversary's behavior. Any randomness thrown in the mix threatens the accuracy and efficacy of the analytical prediction, which in turn makes an analyst uncomfortable. Al-Qa'eda today resembles more of a decentralized movement than a hierarchical organization, particularly following the U.S. military operations in Afghanistan. One could characterize al-Qa'eda post-2001 as a "venture capitalist" terrorist enterprise that grants seed money for semi-independent terrorist operations,[158] or a transnational terrorist franchise that adopts pre-existing groups under its umbrella.[159] A broad-based, decentralized movement will exhibit a higher degree of randomness in its behavior than a unitary organization. The absence of a safe haven replete with training camps, compounded by limited communications with bin Laden's central command element, has devolved al-Qa'eda's operations. Geographically dispersed cells and operatives of varying skill levels and resources will plan and execute attacks that may deviate from the "standard" al-Qa'eda model,[160] so the analyst must anticipate some degree of randomization. Such an anticipation, however, may induce a

[155] *Rational* in this sense means the actor will pursue logical steps to maximize his gain or achieve a certain goal.

[156] Jason Burke, *Al-Qaeda: The True Story of Radical Islam* (New York, NY: I.B. Tauris & Co. Ltd., 2004), p. 15.

[157] Conversely, it has become fashionable lately to presume terrorists belong to a wholly decentralized network. In either case, preconceptions and assumptions can lead to faulty conclusions.

[158] Burke, p. 13.

[159] Fred Burton, "Al Qaeda in 2006: Devolution and Adaptation." *STRATFOR* (Strategic Forecasting, Inc.), 3 January 2006, http://www.stratfor.com/products/premium/print.php?storyId=260353 (accessed 18 February 2006).

[160] Fred Burton, "Beware of 'Kramer': Tradecraft and the New Jihadists." *STRATFOR* (Strategic Forecasting, Inc.), 18 January 2006, http://www.stratfor.com/products/premium/read_article.php?id=261022 (accessed 16 February 2006).

third type of bias, one that has recently gained prominence in the antiterrorism community. It stands as the antithesis to the centralization bias.

Since al-Qa'eda lost its Afghan safe haven, many analysts regard the Islamist global jihad as a completely decentralized network, devoid of any significant command structure or hierarchical elements. The global network paradigm has garnered champions throughout the counterterrorism community, academia and the public policy arena.[161] The network concept, however, demands a nuanced analytical approach, one that is often ignored in public discourse in favor of broad generalizations. Such generalizations about networks—generalizations that conflate networked structure with the concept of decentralization—can foster an incomplete understanding of the complex terrorist apparatus and yield imprudent counterterrorism policy options and terrorism countermeasures.

Assertions that al-Qa'eda has become a dispersed, decentralized network are overly simplistic and ignore the uneven nature of the global jihad and its participants. Al-Qa'eda may have decentralized after 2001, but not necessarily to a uniform degree across

[161] For further reading on the al-Qa'eda network, terrorist networks and network analysis, the debate on centralization and decentralization, and organizational dynamics and network theory in general, see John Arquilla and David Ronfeldt, "Networks, Netwars, and the Fight for the Future," *First Monday*, vol. 6, no. 10 (September 2001), http://www.firstmonday.org/issues/issue6_10/ronfeldt/ (accessed 19 May 2006); Jacob N. Shapiro, *Organizing Terror: Hierarchy and Networks in Covert Operations* (Working paper, Stanford University, 1 November 2005); Malcolm K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks*, 13 (1991): 251-274; Major Troy S. Thomas, USAF, *Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism* (Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004), pp. 157-158; *MetaMatrix: Tools for the Analysis of Organizational Structure*, http://casos.isri.cmu.edu/projects/MetaMatrix/index.html (accessed 6 June 2006); Kathleen M. Carley, *Estimating Vulnerabilities in Large Covert Networks* (Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d.) http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/249.pdf (accessed 6 June 2006); Stephen P. Borgatti, Kathleen M. Carley and David Krackhardt, *On the Robustness of Centrality Measures under Conditions of Imperfect Data* (Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d.), http://www.analytictech.com/borgatti/papers/robustness.pdf (accessed 6 June 2006); Valdis E. Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24 (3): 43-52, http://www.insna.org/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf (accessed 17 May 2006); Michael J. Hannan, LCDR, USN, "Operational Net Assessment: A Framework for Social Network Analysis," *IOSPHERE* (Fall 2005):27-32, http://www.au.af.mil/info-ops/iosphere/iosphere_fall05_hannan.pdf (accessed 6 June 2006); Linton C. Freeman, "Centrality in Social Networks: Conceptual Clarification," *Social Networks*, 1 (1978/79): 215-239; Noah E. Friedkin, "Horizons of Observability and Limits of Informal Social Control in Organizations," *Social Forces*, vol. 62, no. 1 (September 1983): 54-77; Gary J. Miller, *Managerial Dilemmas: The Political Economy of Hierarchy* (New York, NY: Cambridge University Press, 1992); Raymond E. Miles and Charles C. Snow, *Organizational Strategy, Structure, and Process* (New York, NY: McGraw-Hill, Inc., 1979); Frank Harary, Robert Z. Zorman and Dorwin Cartwright, *Structural Models: An Introduction to the Theory of Directed Graphs* (New York, NY: John Wiley & Sons, Inc., 1965).

the whole organization. Parts of the old guard—the High Command, the central core—remains as a hierarchical entity, as do some outlying cells and affiliated groups. The central leadership still strives to direct the operations and manage the behavior of its subordinate cells and affiliates. The level of control that it wields varies across the network, contingent on how tightly connected the core is to the respective cells. When analysts predispose themselves to regard the jihadi network as fully decentralized, or even leaderless, they may fail to recognize key cells or individuals (called *nodes* in the network) that exert greater-than-average influence on terrorist activities. Key nodes may include ideologues, terrorist organizational leaders, financiers, logistical facilitators, or even heads of sympathetic states. Targeting critical nodes in the network may reduce its effectiveness, hinder its communications, or even thwart an attack. Sometimes isolating a key member from the rest of the network (see Figure 8) may force the apparatus to adapt by activating redundancies—new, substitute nodes that analysts had not previously identified (as in Figure 9), or new links between nodes to get around the imposed isolation (as in Figure 10).

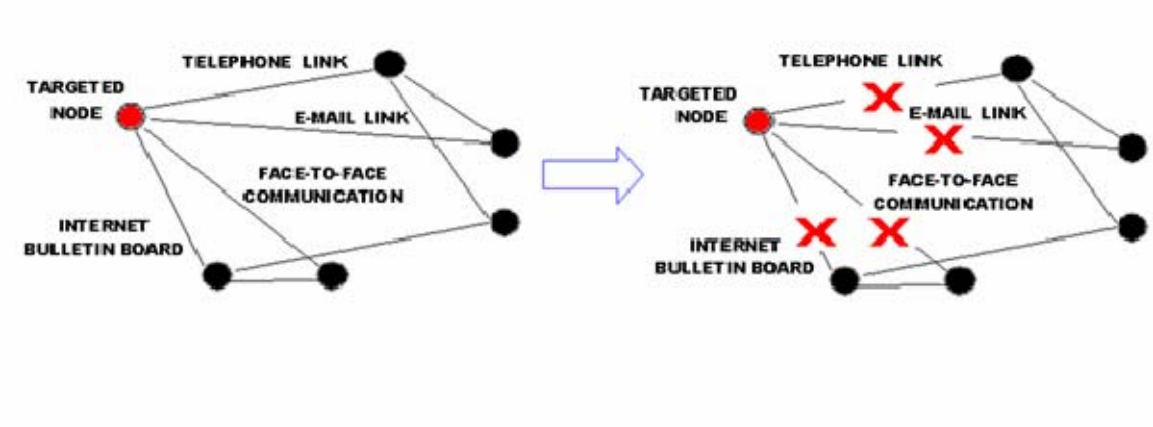

Figure 8 Isolating a Key Node

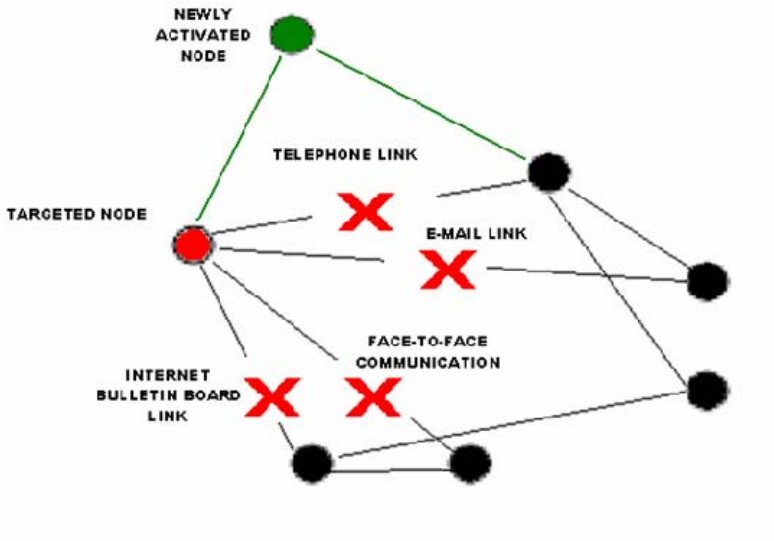

Figure 9 Newly Activated, Previously Unknown Node

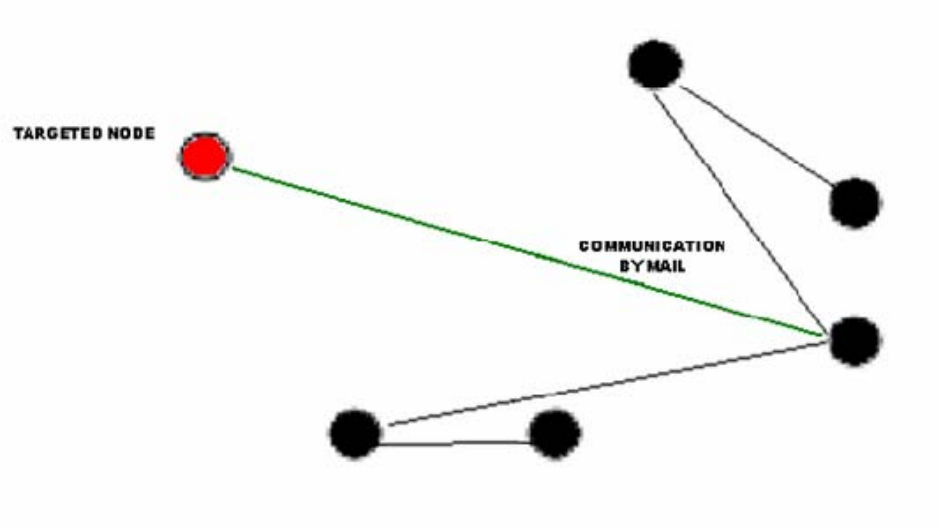

Figure 10 Newly Activated, Redundant Link

The decentralization bias can improperly influence how analysts map a part of a terrorist network. Intelligence reports may identify cells or individual actors as network nodes, and the relations between them as links, but the analyst must understand the substance of the links to assign relative importance to the nodes. One node linked to many others may appear important—a key node worthy of targeting for removal or isolation—but the links may be trivial in value, while another node, seemingly remote

from the network, may exert stronger influence on the terrorist apparatus as a whole. For example, senior al-Qa'eda ideologue Mustafa Setmariam Nasar, alias Abu Mus'ab al-Suri, has only one known link to the al-Qa'eda apparatus. His apparent disconnectedness originally led analysts to underestimate his importance.[162] The substance of a node's links to the network may identify him as a central power broker, perhaps even a chief in a hierarchical terrorist organization, that makes him a worthy counterterrorism target.

In other cases, the hard-core terrorist apparatus may rely on peripherally connected individuals or groups to provide crucial services, such as transfer funds or materiel on the terrorists' behalf. Such individuals, while playing an important role in the network's function, may have weak or even ambiguous loyalties to the jihadi cause. Authorities may be able to co-opt them, wittingly or otherwise, in order to impede network operations. Authorities may also exploit identified cleavages between different cooperating sub-groups with competing parochial agendas. Analysts can recognize these sub-groups by considering the terrorist network is not necessarily an amorphous, leaderless enterprise. An organization need not function exclusively as either a decentralized network or a centralized hierarchy. John Arquilla, David Ronfeldt and Brian Jackson of RAND support this paradigm. Arquilla and Ronfeldt note that in "hybrids of network and hierarchical forms of organization…traditional hierarchies may exist inside particular nodes in a network."[163] Jackson highlights the violent environmentalist movement, which appears at the national level to be a leaderless, loosely connected network. Yet individual "cells within the movement…will have their own authority structures with much tighter [interconnectedness]."[164] Marc Sageman's analysis of the pre-9/11 global jihad network indicates the Southeast Asian cluster (*Jemaah Islamiya*, or Islamic Group) represented more of a hierarchy than the other

---

[162] Jarret M. Brachman and William F. McCants, *Stealing Al-Qaida's Playbook* (West Point, NY: Combating Terrorism Center, February 2006), p. 15.

[163] John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)" in *Networks and Netwar: The Future of Terror, Crime and Militancy*, eds. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), p. 8.

[164] Brian A. Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda," *Studies in Conflict and Terrorism*, 29 (2006): 249.

elements.[165] Ultimately, an analyst must walk a balance beam between the two biases of seeing things as purely hierarchical, or seeing them as completely decentralized. Either predisposition will blind the analyst to exploitable, subtle details in the global jihad.

The popular paradigm of a decentralized global network presents a noteworthy pitfall. Arquilla and Ronfeltd introduce a concept called network-centric warfare, or "netwar," in which they describe how a hostile, decentralized network can execute coordinated attacks. They, along with Michele Zanini and Sean J.A. Edwards, argue the best way to combat a decentralized amalgam waging network warfare is to employ decentralized netwar in response.[166] Arquilla and Ronfeldt further propose a shift "away from notions of 'central' intelligence" toward intelligence networks, modeled off the success of business networks, wherein critical information can flow quickly between different subordinate elements.[167] They seem to suggest that "central" intelligence somehow equates to vertical channeling at the expense of broad dissemination. Indeed, horizontal information sharing has its merits, but should not constitute a substitute for aggregated intelligence pooling and analysis. The 9/11 Commission recognized that centralized analysis is critical to recognizing patterns among isolated pieces of raw intelligence.

Ironically, the mandate to "connect the dots" draws the analysts toward yet a fourth bias, the tendency to see patterns in purely random phenomena. The human mind instinctively seeks order. It attempts to frame the world in a logical way, and will "easily misconstrue random events as nonrandom, perceiving a pattern where, in fact, none exists."[168] By construing patterns, the mind can adapt to the world, reacting in established ways to circumstances that resemble familiar ones from past experience. This

---

[165] Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: University of Philadelphia Press, 2004), p. 140.

[166] Michele Zanini and Sean J.A. Edwards, "The Networking of Terror in the Information Age," in Networks and Netwars, eds. John Arquilla and David Ronfeldt (Santa Monica, CA: RAND, 2001), pp. 54-55.]; John Arquilla and David Ronfeldt, "The Underside of Netwar," Review – Institute of Public Affairs (December 2002): 3. Ironically, netwar's presumed strength is in its asymmetry against western government's hierarchical, bureaucratic design. In this case, they recommend using network-centric countermeasures against a terrorist network, and while Zanini and Edwards caution against "mirroring the opponent," they essentially advocate an organizationally symmetric government response.

[167] Arquilla and Ronfeldt, "Underside," p. 3.

[168] Morgan D. Jones, *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving* (New York, NY: Three Rivers Press, 1998), p. 18.

way the mind doesn't have to evaluate each situation in detail, but can apply mental shortcuts to select behaviors that proved effective in similar, past situations.[169] These mental shortcuts normally serve humans well, but they can prove dangerous for the intelligence analyst.

Intelligence consumers expect the analyst to identify patterns in the chaos of raw field reporting. After all, discerning the pattern is the first step in the analytic process, the bedrock of finished intelligence assessments. Consumer expectations, combined with the natural bias, can lead analysts to find non-existent patterns in truly random events, which could foster erroneous intelligence judgments and predictions. The terrorism analyst must remain acutely cognizant of this natural mental bias. Perhaps the best way to minimize its effects is to seek data that do not fit the pattern; when enough information falls outside the perceived pattern, the analyst may conclude the behavior or events under consideration are indeed random. If he cannot find enough evidence to discredit the pattern, the analyst can improve his confidence that an actual pattern does exist. Precisely how much data the analyst will need to make such a determination is really up to the analyst, contingent on how much overall information is available. A larger sample of data (such as numerous case studies) will help lift true patterns above the random clutter.[170]

I. THE VOLUME CHALLENGE

Making more information available to analysts doesn't always yield better intelligence assessments. Richards J. Heuer, Jr., conducted extensive research into the methodologies and psychological underpinnings of intelligence analysis during his tenure at the CIA's Directorate of Intelligence. He highlights studies which suggest an intelligence analyst's "judgments are determined by a few dominant factors, rather than by the systematic integration of all available information."[171] Once an analyst has formed his estimate from a given set of evidence, additional information won't

[169] Jones, p. 22.

[170] Heuer, pp. 120-122.

[171] Ibid., p. 52.

necessarily improve its quality, but will increase his confidence in the estimate (unless the additional information discredits his initial analysis, in which case the analyst's confidence should decrease).[172]

While offering an analyst more information may not contribute to better analysis; it may foster the opposite effect. The 9/11 intelligence failure, from the standpoint of inadequate analysis, highlighted a major obstacle analysts face in the Intelligence Community. Part of the problem stemmed from the tremendous volume of available information. The Intelligence Community gathers thousands of field reports daily on topics ranging from Chinese military capabilities, to economic developments in Nigeria, to terrorist activities in Colombia. The law enforcement community, even less interconnected than the national Intelligence Community, gathers information from countless crime reports and investigative activities, only some of which can rightly be labeled intelligence. Trying to sift through mountains of seemingly disconnected data and trying to find substantive links is a daunting challenge. The post-9/11 inquiries suggested the "first issue in intelligence gathering focuses…on the sheer volume of information." Today within the law enforcement and intelligence communities, "the simple fact is there is too much information [which] is useless unless it is analyzed."[173]

An analyst must sort through high volumes of raw intelligence reporting, attempting to extract relevant details of information from disparate sources and field reports, while simultaneously digesting it all as a coherent whole so as to discern larger patterns or detect anomalies. This has been called the "wheat versus chaff" problem, where the analyst attempts to winnow choice morsels of information ("wheat") from a larger body of extraneous data ("chaff"). The phenomenon has also been dubbed the "signal versus noise" challenge; the information that may contribute to the analysis, or "signal," hides amidst a much larger "noise" volume of lesser value.[174]

---

[172] Heuer, p. 52.

[173] Jonathan R. White, *Defending the Homeland: Domestic Intelligence, Law Enforcement, and Security* (Canada: Wadsworth/Thomson, 2004), pp. 23-24.

[174] It is only of relatively lesser worth in that the overall larger sample of "noise" may present grand patterns for the analyst that will not be evident in the smaller samples of details. (See Lowenthal, p. 114.)

J. AUTOMATED ANALYTICS AND DATA MINING

Information databases and computerized analytical algorithms (called analytics) provide analysts a powerful tool in predictive analysis, especially when facing a data overload. Automated data processing systems can evaluate significant volumes of information stored in multiple databases, and do so quickly. This process of cross-referencing data elements to discern patterns, links and associations is called *data mining.* Information databases can be extremely large and complex. Combing various databases and performing link analysis between all the data points might take a human analyst weeks, while a computer could do it in minutes. "With data mining," notes Colleen McCue of the Research Triangle Institute, "we can perform exhaustive searches of very large databases using automated methods, searching well beyond the capacity of human analysts or even a team of analysts."[175]

Automated programs need a human analyst to feed the system properly. Field collectors (patrolmen or plain-clothed investigators) submit field reports to a central clearinghouse. The analyst therein must sift through the reports and extract pertinent data that fit categories in the analytic database. He must then translate those data into a usable format for the computer system and input them. An analytic database is generally unable to extract the appropriate data directly from the field report. The analyst must interpret the report for the system.[176] He feeds various data fields in the system, such as location, time, subjects' names, and passport information (country of origin, date and place of issue, passport number—whatever the officer gathered for his field report). Automated data mining systems pool disparate pieces of information, giving the analyst ready access to all of it in one place. An automated search can identify the data commonalities between different databases—a potentially difficult and time-consuming process for a human analyst. Appendix C illustrates how such a process should work.

Computerized analytical algorithms offer another advantage in that they are normally free from cognitive bias.[177] Computers perform numerical calculations.

[175] Colleen McCue, "Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism," *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 47-48.

[176] Khalsa, p. 21.

[177] This presumes the programmer designed the algorithm without a case-specific mindset that induced him to weight certain factors unfairly over others.

Human analysts tend to employ qualitative judgments, which rely on intuition and therefore are more susceptible to cognitive bias. If an analyst can design an analytical model using quantitative inputs, a computer can arguably generate more accurate results than intuitive cognitive approaches.[178] Essentially, computers excel at data-driven analysis. Critical for their accuracy, though, are a solid conceptual model and accurate data inputs with appropriately assigned quantitative values.

Programmers have recently developed software uniquely suited to terrorism analysis, particularly regarding Islamist terrorism. Ordinary databases have limited capability to detect potential name variations and link them to a given person. Arabic names[179] can transliterate into multiple romanized forms, as illustrated by the humorous truism that *Muammar Kaddafi* can be spelled two thousand different ways. Terrorist operatives have used this to advantage by altering their names for different documents, thereby masking their movements and identities. Consider, for example, the name of this obscure Saudi Arabian terrorist:

Osama bin Laden

His name, broken down, is:

Osama (given name) *bin* ("son of") *Laden* (surname)

A more complete rendition would be:

Osama bin ("son of") *Muhammad* (father's given name) *bin* ("son of") *Laden*

A full rendition would be:

Osama bin Muhammad bin Laden al-Yemeni (tribal origin, literally, "the Yemeni")

[178] Khalsa, p. 13.

[179] Islamist terrorists should generally have Arabic names, regardless of their nationality, since dutiful Muslims are supposed to take Arabic names.

Numerous permutations are acceptable, as *bin* can also be written *ibn*, and as it is extraneous, it can be left off altogether:

Osama ibn Muhammad ibn Laden al-Yemeni
Osama Muhammad Laden al-Yemeni

Further permutations include *Osama Laden*, *Osama Muhammed Laden*, *Osama al-Yemeni*, etc. Variations in romanization yield even more alias possibilities:

Usama bin Muhamed bin Ladin, *Osama ibn Mohammed ibn Laden el-Yemeni*, etc.

A wily operative may enter the country on a passport as *Osama bin Laden al-Yemeni*, obtain a student ID card as *Osama B. Laden*, and apply for a driver's license as *Usama A. Yemeni* (since the driver's license only has three name fields in which to fit five apparent names: *Osama Bin Laden Al Yemeni*).

Special software can cross-reference name databases. An algorithm identifies potential name permutations that may link to one or more individuals.[180] It then flags the data for the analyst, who may initiate an investigative follow-up. If multiple name variants seem linked to one individual, it may indicate possible deception on his part: he might have changed his name's appearance to hide his activities. Not surprisingly, the 9/11 Commission found that the nineteen hijackers had used 364 aliases between them, some of which included "different spellings of their names."[181]

The 9/11 hijackers used a time-proven technique to avoid detection by authorities. In 1990, Egyptian Sheikh Omar Abdel Rahman,[182] known as the "blind sheikh," used a name variant on his I-94 immigration entry form to visit the United States. (It was a variation of the name on his passport.) Three weeks earlier, the Immigration and

[180] First Technologies, LLC., "Understanding Islamist Militant Terrorism and Prevention Strategies," Federal Law Enforcement Training Center, Glynco, GA, 16-17 September 2004.

[181] Thomas R. Eldridge, *et al.., 9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: 2004), 911_TerrTrav_Monograph.pdf as an electronic file, p. 1, citing CIA analytic report, "Name Variants and Aliases of 11 September Hijackers and Associates," March 2004.

[182] Rahman was later convicted for his involvement in the first World Trade Center bombing of 1993.

Naturalization Service had watchlisted Rahman in the National Automated Immigrant Lookout System (NAILS), but the system was unable to reconcile the name on the I-94 with the one in the database, because the "watchlist needed an almost exact name match" to flag him.[183] The State Department later instituted a name-matching system to avoid a repeat of the "Blind Sheikh episode." The State Department developed a "language algorithm…for Arabic, [and] implemented [it] in December 1998. This enabled the system [to] search its records for all variant spellings of, for example, the name 'Mohammed.'"[184] (Unfortunately, a proprietary system equipped with such software, used by only one federal department, provides little security against operatives who use name variants to apply for state driver's licenses, rent apartments, open utilities accounts or enroll in flight schools, and are thereby able to melt untraceably into society.)

Automated analytic tools represent a powerful asset in an analyst's arsenal, but one must caution against relying too heavily on computers at the expense of human involvement. A computer data-mining algorithm can identify patterns and linkages—even trends—but it cannot ascertain the significance of such findings. The skilled human analyst must put it all into context.[185]

K. STRUCTURING LAW ENFORCEMENT INTELLIGENCE ANALYSIS FOR ANTITERRORISM

Police departments lucky enough to have a narcotics, gang or organized crime unit often enjoy a pre-existing analytical capability, since these types of crime generally involve a continual management of criminal intelligence. A truly robust analytical capability, however, takes more than skilled individuals in a single police department. A structured system of interconnected analysts offers the law enforcement community the greatest leverage. Cooperative arrangements particularly empower smaller departments or other agencies that may not be "able to staff full-time criminal intelligence units."[186] Regional networks, like the High Intensity Drug Trafficking Area (HIDTA) system, the Regional Information Sharing Systems (RISS), or the El Paso Intelligence Center (EPIC)

[183] Eldridge, *et al*., *9/11 and Terrorist Travel*, p. 51.

[184] Ibid., pp. 80-81.

[185] Jeffrey W. Seifert, "Data Mining: An Overview," *The Library of Congress CRS Report RL31798* (Washington, DC: Congressional Research Service [CRS Web], 7 June 2005), p. CRS-3.

[186] D. Douglas Bodrero, "Law Enforcement's Challenge to Investigate, Interdict, and Prevent Terrorism," *The Police Chief* (February 2002): 45.

already have the infrastructure in place for intelligence sharing. These networks can easily facilitate terrorism information and analytical collaboration as well.[187] Furthermore, the current Joint Terrorism Task Forces and the emergent state and regional fusion centers will pool analytical assets (and enjoy a healthy investment of federal analytical capability) specifically aimed at terrorism.

Those organizations with the budget and manpower to establish analytical offices still need to network vertically and horizontally. Analysts from various localities and regions evaluate patterns and trends in their jurisdictions, and share the intelligence with other jurisdictions and echelons in the network, as depicted in Figure 11. Seemingly isolated events in one locality may in fact represent a pattern across a wider geographic area.

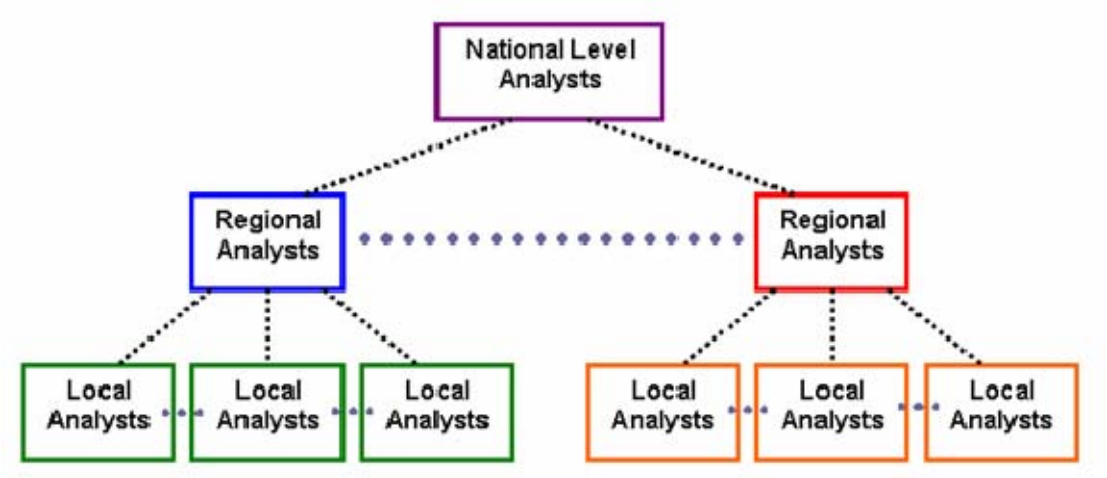

Figure 11 Layered Analytical Network Structure

Suspected surveillance may become part of a larger picture when assessed alongside similar reports of train station surveillance in Montgomery, Alabama and Savannah, Georgia. (See Figure 12.) The regional analyst can alert the various localities in his area of responsibility, inform them about this pattern, and discharge them to look for additional surveillance in their respective jurisdictions. With this new lead to follow, police in Charleston, Tallahassee and Mobile may soon discover rail surveillance in their cities and report it to the Atlanta regional office.

[187] Bodrero., pp. 45-46.

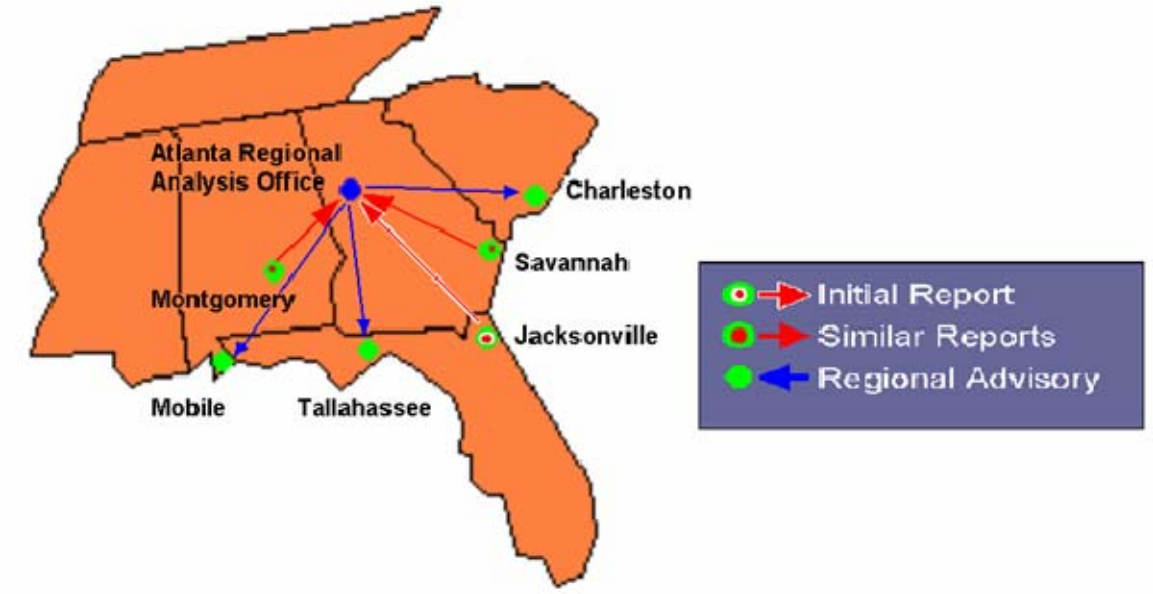

Figure 12 Regional Analytical Cooperation

Analysts in the various jurisdictions can horizontally share information, compare assessments, and cross-levy collection requirements. Police in Mobile can have their analyst query his counterpart in Savannah about the type of vehicle the surveillants used in their area, or the number of people seen surveilling the train station at a given time. The key is to keep the communication and information flowing to facilitate a broad analytical enterprise.[188] Al-Qa'eda has demonstrated its intent and ability to strike multiple, geographically separated targets, nearly simultaneously. If the terrorists are coordinating attacks over wide areas, the law enforcement organizations must also. Regional cross-fertilization compounds the value of terrorism intelligence analysis.

L. HARNESSING ANALYSIS FOR THE FUTURE

Law enforcement agencies today recognize the need to gather intelligence if they hope to interdict terrorist operations in the United States. The so-called intelligence failure of 11 September 2001, however, revealed that massive quantities of information were insufficient to thwart a terrorist attack; inadequate analysis proved to be the Achilles' heel for the national Intelligence Community—a lesson the law enforcement

[188] One must distinguish this from simple *information sharing*, which can take the form of broad "shotgun" dissemination of raw field data without necessarily applying analysis. Networked analysis implies a sharing of information and a cooperative team approach to analyzing that information.

community should take to heart. Analysis lends significance to collected information, thereby informing intelligence consumers who use it to craft policy, select defensive countermeasures, plan investigations and operations, or collect further intelligence. The analyst provides the consumers with a picture of the aggressors and the threat—both a description of the present circumstances and a forecast of possible future events. This forecasting is the lynchpin of terrorism analysis: it aims to interdict terrorist attacks and save lives. Therefore, analyst accuracy is crucial. Certain mental biases can encroach on that accuracy, however. An analyst must be cognizant of the biases and work to reduce their effect on his analytical judgments.

Furthermore, an analyst must wrestle massive amounts of data, risking information overload that may overwhelm his analytical abilities. A few automated analytic tools are available to collate mountains of data and identify potential links between data elements (including multiple foreign name variants used by individual terrorist suspects). Automated tools, though, are just that—tools. The machines still require a skilled human analyst to feed them and interpret their outputs.

A strong terrorism analytical capability does not reside in a single, isolate police intelligence unit. A truly effective program must be structured across the law enforcement community, tying together analysts from multiple jurisdictions and echelons, from the local, through the regional, and up to the national level. An integrated analytical network[189] enables information sharing, cross-jurisdictional information queries, and, most importantly, the recognition of terrorist behavior patterns dispersed across a broad geographical spread—patterns not observable from isolated local jurisdictions. The terrorists are dispersed but networked. The law enforcement intelligence community must follow suit.

[189] Having an integrated network does not imply a completely decentralized, leaderless law enforcement apparatus. Police agencies are themselves, by nature, hierarchical. Higher echelons must have some means to coordinate lower-level analytical efforts and manage the overall process in an organized regional or national effort.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COVERING ASSETS: INTELLIGENTLY FOCUSED DEFENSIVE ACTIONS

Intelligence collection and analysis for its own sake serves little purpose. To have value, it must inform the planners and decision-makers who select courses of action to mitigate terrorist threats. Terrorist threat intelligence simply forms the baseline for further action.

Proper antiterrorism security planning requires good threat intelligence. Security planners must know the terrorists' capabilities, tactics and intentions in order to evaluate asset vulnerabilities in the proper context. From there, they can tailor defensive measures accordingly. An antiterrorism plan built in an intelligence void, however, risks protecting the wrong assets, or hardening the wrong resources improperly or incompletely. Threat intelligence frames a coherent risk assessment, which in turn helps planners prioritize their defensive expenditures and select rational countermeasures.

"The Department of Homeland Security (DHS) is responsible for establishing the risk management framework necessary to coordinate" federal efforts "to identify and prioritize the United States' critical infrastructure and key resources (CI/KR)" that require protection from terrorists.[190] DHS has aggregated nearly 80,000 assets in a single comprehensive list, the National Asset Database (NADB), but currently lacks "the data and the analytical tools to provide a comprehensive risk assessment of the country's critical infrastructure and key resources."[191]

Asset prioritization and protection responsibilities traditionally defaulted to local jurisdictions and the private sector, but the current push for a national program blurs the distinctions between federal, state and local interests. Nearly 50,000 items in the NADB are not federal assets, but submissions from the states and territories.[192] The criteria for nomination varies from state to state, fostering significant disparities in what states

[190]U.S. Department of Homeland Security Office of the Inspector General, "Progress in Developing the National Asset Database." [OIG Report] *OIG-06-40* (Washington, DC: U.S. Government Printing Office, June 2006), p. 1.

[191] Ibid.

[192] Ibid., p. 6.

consider "critical."[193] The federal government now must reconcile the asset list with a standardized risk assessment process, essentially assuming a planning responsibility previously exercised at lower echelons. While a seemingly overwhelming task, this new approach offers some advantages. Islamist terrorists, as noted in the Methodology and Analysis chapters, do not confine their operations to a single jurisdiction. A multi-layered analytical construct stands better suited to recognize and evaluate geographically dispersed activity, and can assist national antiterrorism planners apply uniform risk assessment tools, resource prioritization schemes and asset protection measures across the country. Ideally under such a nation-wide regimen, a terrorist cell targeting a shopping mall in Seattle will fare no better by switching its focus to one in Memphis, and a cell won't find it easier to attack a nuclear power plant in San Diego than a bus stop in Chicago.

The federal government, states, territories and local jurisdictions all must adopt a set of standards for evaluating assets as potential terrorist targets. Armed with accurate threat intelligence, each echelon can make rational, though somewhat subjective, risk assessments. DHS has promulgated an tool called the Criticality Assessment Matrix, but a full risk analysis requires additional inputs. This chapter proposes one comprehensive methodology, the Multi-Matrix Method, that combines intelligence inputs with the Criticality Assessment Matrix. Planners at any level, from local to federal, may find the Multi-Matrix Method useful for assessing risks to assets and prioritizing risk mitigation efforts.

A. THREAT-BASED ASSESSMENTS AND PLANNING

It might appear redundant to suggest that one must ascertain the specific nature and magnitude of the terrorist threat before evaluating a target's potential vulnerabilities or developing security countermeasures. However, people overlook this basic concept so often it warrants emphasis. Time and again owners and users responsible for securing a resource (or protecting personnel) implement procedures without defining what specifically those actions should accomplish. Usually they resort to familiar measures

[193] U.S. Department of Homeland Security Office of the Inspector General, p. 6; Pam Fessler, "Homeland Security Asset Report Inflames Critics," *All Things Considered* (12 July 2006), http://www.npr.org/templates/story/story.php?storyId=5552554 (accessed 7 November 2006); MSNBC, "Inspector: Homeland Security Database Flawed," *MSNBC News Services* (12 July 2006), http://www.msnbc.msn.com/id/13822662/ (accessed 7 November 2006).

that may have been effective against another threat encountered once in the past, but do not carefully consider the current threat. These measures are sometimes called "knee-jerk" reactions.

Analysts assume the chief role in combing through available intelligence, taken in historical context, to approximate qualitatively what threat a terrorist group likely poses. This qualitative analysis should consider the group's resources, such as money, personnel, weapons and materiel, to assess its capabilities. The analysis must take into account the group's intentions, based on the group's publicly stated targeting goals, as well as those gleaned from informants and a careful assessment of the group's historical activities. This historical piece is critical, as it places any potential threats into proper context. A group that for years has only attacked deserted ATM booths with pipe bombs is unlikely to escalate suddenly to sarin gas attacks against populated areas, even if the new terrorist leader issues a manifesto publicizing such a threat.[194]

A proper security plan hinges on a good risk assessment, which takes into account the likelihood of a given attack, and the potential severity of the damage a successful attack may inflict.[195] A proper understanding of hostile threats and a resource's vulnerabilities informs the risk assessment.

The threat evaluation begins the entire process, and it must precede the vulnerability assessment. One can only ascertain an asset's vulnerability in light of a given threat. An ordinary automobile will protect its passengers from knife-wielding thugs; the passengers can be said to be relatively invulnerable. If one of the thugs possesses a gun, however, the same automobile affords little protection; the passengers are assessed to be quite vulnerable. Nothing is completely invulnerable. Assets are only

[194] One should not discount the possibility that the threat may evolve to adopt new methods, but such changes are generally heralded in intelligence by subtle indicators. Even the use of airliners on 9/11 was not novel: Islamist plans to use aircraft in kamikaze missions date as early as 1989. See Gus Martin, *Understanding Terrorism: Challenges, Perspectives, and Issues* (Thousand Oaks, CA: Sage Publications, Inc., 2003), p. 236; Paul R. Pillar, "Fighting International Terrorism: Beyond September 11th," *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 19; Joseph S. Bermudez, Jr., *Terrorism: the North Korean Connection* (New York, NY: Crane Russack [Taylor & Francis New York, Inc.], 1990), p. 83.

[195] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York, NY: Copernicus Books, 2003), p. 20.

vulnerable or secure relative to a specific number of threats. Pinpointing the threat proves necessary before one can adequately evaluate a resource's security strengths and weaknesses.

1. Threats, Vulnerabilities and Countermeasures

The assessment process requires a thorough understanding of the danger the adversary poses: what he wants to do (how he can attack), what he can do (his capabilities), and what he intends to do (his ultimate plans), and the three may not be congruent. For example, a terrorist cell might wish to detonate a nuclear warhead in Washington, DC, but does not possess such a device. It may have a biological weapon, with a highly virulent contagion, that it can deploy in a large city. The group may intend, however, simply to detonate a massive truck bomb, laden with conventional explosives, because one of its supporting states has an embassy in Washington and has expressed concern about the collateral damage a bio-weapon would pose to its own diplomatic personnel.

Knowing a terrorist group's capabilities and intentions aids security specialists assess potential targets in context. First, it narrows the likely target pool, which in turn helps the specialists and owner-users harden the appropriate resources. Any police officer will agree that if several neighborhood jewelry stories have been heisted by a ring of diamond thieves, it stands to reason the police should focus the bulk of their defensive efforts on jewelry stores, rather than expend too much effort bolstering security measures for the neighborhood electronics stores, furriers or antique shops. "Overestimating the threat potential means wasting dollars, personnel, time, and effort."[196] In this crime example, treating the threat against other businesses as equal to that faced by jewelry stores would be an overestimation of the threat to the other establishments. The same reasoning applies to antiterrorism efforts. Unfortunately, many people fail to appreciate the necessary link between the threat's qualitative character and the potential targets. One Cold War veteran presumed the nearby nuclear submarine base would be one of al-Qa'eda's top targets.[197] The base probably topped the Soviet Union's target list during

[196] Frank Bolz, Jr., Kenneth J. Dudonis and David P. Schultz, *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*, 2nd Ed. (Boca Raton, FL: CRC Press LLC, 2002), p. 25.

[197] Author's personal conversation with the veteran, ca. 2003.

the Cold War since nuclear counterstrike forces were a top priority for them, but realistically it was too far from a significant population center and too heavily fortified to make al-Qa'eda's list. The terrorist threat al-Qa'eda poses today differs significantly from the strategic nuclear threat the Soviet Union presented twenty years ago.

The threat study helps planners prioritize targets needing their attention, and also informs them about likely attacks against which they must protect, giving them a baseline for evaluating each target's vulnerabilities. "Target or threat analysis includes not only the likelihood of becoming a target, but also whether or not offered defenses are sufficient to discourage attacks"[198] or limit the damage they may inflict. This step is iterative, in that one must analyze the asset's current security measures in light of the threat; once the planners select additional measures to address any security weaknesses, they must re-evaluate those measures to determine if they will, in fact, reduce the vulnerabilities and mitigate the threat. Carefully re-examining the nature of the threat and comparing it to proposed antiterrorism countermeasures will normally disclose whether the security actions can effectively address the threat. Often decision makers overlook this comparative "check step" when selecting defensive measures.[199]

When denied the luxury to take the time to evaluate the threat, brainstorm appropriate countermeasures, and consider their effectiveness against that threat, security planners often fall prey to the unconscious misconception that inconvenience equals security. They may also implement familiar measures that might be suitable for one kind of threat (such as ordinary crime), but notably inappropriate for the threat in question (terrorism). Installing metal detectors and X-ray machines at a building's entrance might prevent a person from smuggling a weapon into the facility, but if the predominant terrorist MO is to park a truck bomb in front of the building, the security measures will prove inadequate.

This example underscores how important it is to base antiterrorism and security processes on a thorough threat analysis. Terrorists do not act randomly, nor do they act capriciously or spontaneously. Rather, they carefully select targets, plan their attacks,

[198] Bolz *et al.*, p. 26.

[199] Schneier, p. 14.

and generally continue to use weapons and methods that have served their purposes well in the past. Most generic security procedures have been designed to protect against common criminal threats, which often consist of spontaneous criminal acts against targets of opportunity. Muggers prey on random victims in dark alleys and streets. Terrorists do not; they orchestrate carefully planned operations against select victims, which means common anti-crime measures may not thwart their designs.[200]

2. Ulterior Motives

A poor understanding of the threat can foster poor security choices in another way. People sometimes implement improper defensive countermeasures based on an alternative agenda, one not related to security or antiterrorism. They may capitalize on a security issue to introduce potential security solutions that satisfy the non-security agenda.[201] A good threat assessment will enable security planners to evaluate the potential solutions' efficacy, and to discard any that do not appropriately mitigate the threat.

3. Collateral Consequences

An antiterrorism plan does not simply end with selecting good security countermeasures. The measures may introduce side effects or unintended, collateral consequences. These unintended consequences can take two forms: they may have spillover effects not directly related to security,[202] or they may introduce new security vulnerabilities to the resource in question or other resources.[203] An armored car may be the ideal solution to protect a motorist from carjackers carrying firearms. Armored cars naturally weigh more than ordinary cars, necessitating a larger engine which burns more gasoline. An unintended spillover effect, then, is the increased fuel consumption and

[200] Terrorists do not target randomly; they prefer to appear deliberate in their targeting. "Very few acts of terrorism…are meant to appear indiscriminate. Terrorists normally want to appear selective [because while] indiscriminate violence may produce greater fear and alarm among the general population, selective but unpredictable attacks may cause greater alarm within the selected group." The terrorists may choose a target carefully, such as a building, business or event, but don't care about who actually gets killed in the event (via collateral damage or mass targeting). Thus, the violence appears random or indiscriminate. See Brian M. Jenkins, "International Terrorism," in *Air Command and Staff College* text version 3.2, 9 vols. (Maxwell AFB, AL: Air University Press, 2000), vol. 2: *National and International Security Studies*, p. 238.

[201] Schneier, pp. 33, 38, 41, 279-280.

[202] Philip B. Heymann, *Terrorism, Freedom, and Security: Winning without War* (Cambridge, Massachusetts: The MIT Press, 2003), pp. 59, 101-104, 135-136.

[203] Schneier, pp. 14-15.

concomitant expense. Being heavier, an armored car will have more momentum, thus being be more difficult to handle in tight turns and sudden stops; this poses an additional safety (distinct from *security*) hazard for the driver. Finally, if the driver is commuting in a hostile environment where terrorists target VIPs in armored vehicles, the driver's new car may raise his profile. The terrorists may mistake him for a dignitary and attack him with a rocket-propelled grenade, against which his armor is ineffective. Thus, while his armored car protects the motorist from the original threat—the carjackers—it exposes him to a new threat, the heavily armed terrorists.

A collateral consequence being unintended does not mean it should be unexpected. Good planners must anticipate the potential side effects of any course of action. Consequences must balance with the intended gains; a new security threat that dwarfs the original one should discount a countermeasure's utility. Even if the measure effectively addresses the original threat, it could open up avenues for other threats, drawing the planners into an iterative evaluation process where they must balance multiple liabilities to select the optimal all-around solution.

Sometimes a poor countermeasure choice compounds the issue by creating unintended weaknesses while failing to address the original threat in the first place. This often stems from improperly grasping the threat. Security specialist Bruce Schneier notes, "If you mischaracterize your attackers, you're likely to misallocate your defenses. You're likely to worry about nonexistent threats and ignore real ones. Doing so isn't necessarily a disaster, but it is certainly more likely to result in one."[204]

Consider the following example of off-base restrictions. The U.S. military reaction to September 11th was fairly universal. Overseas commanders, fearing other strikes, locked down their personnel on the installations. Gradually, intelligence and counterintelligence personnel got a handle on the al-Qa'eda threats in their respective localities, and commanders began letting their troops leave the bases to patronize local national businesses, but within certain restrictions. The commanders at one overseas air base[205] initially prohibited their troops from visiting bars or nightclubs. Their rationale

[204] Schneier, p. 41.

[205] Example from the author's professional field experience.

stemmed from two lines of analysis. The first was legitimate: Al-Qa'eda preferred attacking large clusters of Americans to maximize carnage. American troops did not cluster in shops or restaurants in nearly the numbers or density as they did in bars, so shopping and dining establishments were less attractive targets. Keeping troops out of the bars and nightclubs kept them from congregating in numbers that might entice a terrorist attack.

The second line of logic, however, had no grounding in threat analysis: Some people reasoned that inebriated troops were less vigilant and had slower reflexes than sober ones (true), so they would be less likely to notice and recognize an attack in progress, and they would be less capable of reacting to it because of their intoxication (again, true). Thus, they concluded groups of drunken GIs made attractive terrorist targets, and suggested the terrorists actually took this into account during their target assessment. Intelligence uncovered no indication that Islamist transnational terrorists (al-Qa'eda included) considered people's level of intoxication as a planning factor. While the argument is a sound one as far a vulnerability, no intelligence data suggested terrorist operatives would choose a group of drunken Airmen over a group of sober ones, simply by virtue of their relative degrees of inebriation. Rather, the operatives were more likely to take into account raw numbers of patrons, facility structural vulnerability, and ease access for explosive emplacement, without regard to the patrons' alcoholic indulgence. [206]

Prohibiting Airmen from patronizing local bars equated to fewer drunken brawls off-base. Certainly a bar restriction would be a great mechanism to reduce the number of alcohol-related assaults if that were the primary threat for which the security measure was intended. Unfortunately, the commanders implemented the alcohol restriction as antiterrorism measures to protect the Americans from the transnational Islamist terrorist threat. The measures' appeal stemmed not from sound security analysis, but from an alternative agenda.

The early curfew incident had an even darker side. It did not address the actual threat, though it did create a potentially unsafe situation for the troops by presenting a

[206] Keeping people sober is not a bad idea at all, because sobriety does facilitate greater vigilance and clearer thinking; the issue is that it was attributed to threat analysis when it really had no such genesis.

more alluring target for terrorists. The weekend curfew for active duty military personnel, prior to 9/11, was as late as 2 a.m. This meant all personnel had to be back inside the base confines by curfew or, for those renting off-base apartments, inside their homes. Military police patrolled downtown looking for any GIs who might be out past curfew, and they would apprehend any they found.

The new, curtailed curfew was set at 8 p.m. On the surface, this would appear reasonable: keep people off the streets as much as possible to limit their exposure to the threat and reduce the risk. Early curfews can protect people from street crimes—muggings, assaults or rapes—in areas where violent criminals tend to operate at late hours. But this reasoning did not take into account the nature of the terrorist threat. (In fact, a subsequent analysis of Islamist terrorist attack trends from 1998 to 2005 disclosed no attacks between the hours of 2 a.m. and 6 a.m.[207]) Furthermore, the curfew initiative created unintended consequences. Setting an early curfew—especially a very early curfew—created a logjam at the base's main gate, baiting terrorists with a veritable salt lick.

Terrorists do not operate like muggers; they do not wait around until 9 p.m. to come outside, so rushing everyone onto the base early in the evening "before the terrorists come out" isn't an effective strategy. Terrorist organizations like al-Qa'eda—whom the U.S. believed to be the pre-eminent threat at the time—spend months gathering information about their prospective targets, paying particular attention to the times and locations where larger groups of people cluster together (shift changes, communal dining periods, etc.) in exposed or accessible locations. A convenience store directly across the street from the main gate provided an excellent place for terrorist operatives to sit and observe pedestrian traffic through the gate. Any observer could note that just before curfew, a swell of people gathered outside the pedestrian gate, each awaiting his turn to pass through the identification checkpoint. For a 2 a.m. curfew, there will be an appreciable bottleneck of people whose life's mission is to stay out drinking as late as possible. If the curfew is scaled back to 11 p.m., those hard core, bar-hopping "curfew

[207] IntelCenter, *Standing Assessment Brief on Most Likely Future Baseline Level Jihadi Attack Activity*. (Alexandria, VA: IntelCenter, 7 August 2005), http://www.intelcenter.com/qaeda-charts.html (accessed 18 May 2006).

pushers" will gather at the gate at 11 p.m., while the folks who would normally filter through between 11 and midnight, after some mild socializing, would also cluster up at the gate to make the 11 o'clock deadline. Ratchet the curfew back to 8 o'clock, and you have the first two groups bottlenecked at the gate, joined by the casual dinnertime crowd and evening shoppers—folks who would usually filter through the gate between 8 and 11 o'clock. The effect is easy to see: a tremendous backlog of people congregating outside the gate and exposed on the unsecured street, each waiting for a turn through the checkpoint. Earlier curfews create greater congestion, which to a terrorist translates to opportunities for bigger, more sensational mass casualty events. (How easy it would have been to drive an explosive-laden mini-bus right up to the crowd!) As this case illustrates, if one doesn't properly assess the threat, seemingly intuitive security measures can actually become counterproductive.

4. At What Cost?

Sound antiterrorism measures may address the threat, but they incur costs, both monetary and intangible. The planners must weight the costs against the security gains, as they represent trade-offs. These differ from collateral consequences, in that trade-offs constitute a central part of the equation and are not simply side-effects. One would not consider the purchase price of a large ice cream sundae an unintended consequence; a buyer expects to surrender a set amount of his money in order to enjoy a decadent dessert. Getting fat, on the other hand, may rightly be considered an unintended consequence. Sometimes the collateral side-effects are not worth the benefit gained; the joy of eating a sundae may not be worth the extra calories. Nevertheless, even absent the side-effects, the costs at some point will outstrip the gains, such as when the sundae price is too high, or the would-be buyer is too full from supper to enjoy a large dessert. The same holds true for security countermeasures, specifically when the choices are prohibitively expensive or simply exceed what would reasonably mitigate the risk.

The threat and vulnerabilities partly determine the risk to a given asset or resource, including people. Risk is also a function of the likelihood something damaging (a terrorist attack) might occur, and the degree of potential damage the resource could sustain.[208] Property damage may be easily quantified in fiscal terms, as well as

[208] Schneier, p. 20; Bolz, *et al*., p. 32.

secondary effects like lost income that the resource would otherwise earn were it not for the attack. Insurance compensation constitutes yet another economic loss. Potential human casualties may be calculated in simple numbers, but emotional damages become harder to quantify. Sometimes they manifest themselves insidiously in reduced employee efficiency or decreased customer confidence—all tied to future economic losses. Assessing risk in dollar figures makes the decision process straightforward. Weighing security measures' social or economic costs against human lives becomes tricky. How much money should one reasonably spend to protect a hundred lives? Ten lives? Saving lives is worth how much inconvenience?

Assessing the utility of having an armored car illustrates the cost-benefit calculus. An armored car will protect someone from a carjacking—keeping his car from being stolen at gunpoint, and keeping him alive in the chance a given carjacker tries to kill him. Assume the armored car costs $100,000, while a regular car costs 25,000 dollars. Assuming a motorist buys a new car every ten years, he spends either $100,000 on an armored car or $25,000 for a regular car every ten years. At what point would the expense of buying an armored car seem prudent? The point of equal utility would be when the cost of losing regular cars equals the cost of owning an armored car, or 100,000 dollars. That is, a car owner would have to get carjacked four times every ten years for the armored car to constitute a feasible expense (considering only the monetary loss, not the psychological and emotional trauma that come from repeated victimization). Therefore, if carjackings occur with such frequency that a motorist can statistically expect to get carjacked once every 2½ years (which translates roughly to once every 912 days), then getting an armored car warrants the expense. In a city of one million people, a motorist faces this risk when the city suffers 1096 carjackings each day.

Now consider a city of one million inhabitants, in which one person each day gets carjacked. Furthermore, only one motorist gets killed out of every one hundred carjackings. Thus, the chance of any one person being carjacked on a given day is one in a million, or 0.000001. A motorist can statistically expect to have his car stolen in a carjacking once every one million days, or roughly once every 2,700 years. The odds of getting killed are even smaller at one in one hundred million, or 10^{-8}, giving the motorist a statistical expectation of being murdered in a carjacking once in 270,000 years. Since

most motorists don't expect to live 2,700 years, let alone 270,000 years, the armored car doesn't offer much utility statistically speaking. But the motorist may still wish to buy an armored car to avoid dying in a carjacking; the expense doesn't make much sense from a fiscal perspective when considering potential theft, but a risk-averse car owner may still prefer not to leave his life to chance.[209]

Risk ultimately represents the key decisive element in assessing the costs or trade-offs—in determining "Are they worth it?"

B. PLANNING FOR SECURITY: A PROPOSED METHODOLOGY

An arithmetic decision matrix provides planners with a simple mechanism to sort and rank-order multiple competing items. In an antiterrorism context, the items are generally assets that planners wish to defend from potential attack, and the items compete for limited protection resources. Planners may evaluate each component of a comprehensive risk assessment using a decision matrix, from the likelihood terrorists will strike a given target, to the potential harm such an attack may inflict. These components may be further decomposed into sub-matrices to evaluate information inputs in finer detail and to improve the risk assessment's overall objectivity. One potentially useful technique, based on this concept of layered decision matrices, is the Multi-Matrix Method. This methodology capitalizes on an intelligence-based threat assessment and vulnerability assessment to evaluate the relative risk to multiple potential targets, and to do so as objectively as possible.

1. Prioritizing Potential Targets

A risk assessment helps antiterrorism planners balance the costs of security against the potential costs of an attack. The risk assessment guides the planners to prioritize their efforts and expenditures. A risk assessment scope varies in relation to a planner's breadth of responsibility. Private resource owners have a smaller target field; public safety officials have much broader array of assets to protect, usually defined by a geographic jurisdiction or area of responsibility. As the scope of responsibility widens, the number of potential targets grows, thereby increasing the need for prioritization in

[209] The probability simply describes the odds of an event occurring. In this model, all people face the same miniscule odds of being carjacked or killed, yet statistically, each year 365 people have their cars taken at gunpoint, and three people die in carjackings. One should not assume a person must live 2,700 years before he's at risk of being carjacked, or 270,000 years before being murdered by a carjacker.

antiterrorism planning. One cannot protect every asset equally, despite the ideal goal of applying horizontal protection to society as a whole; resources are finite and the potential targets are virtually unlimited.

While it's impossible to protect every asset terrorists could possibly target, not every asset will realistically fall under the terrorists' consideration. The terrorists have limited resources and manpower, too, so they will concentrate on a select pool of assets to evaluate for potential targeting. Therefore, one would ideally concentrate defenses on those potential targets the terrorists find most attractive—ideally, the very same target list the terrorists have compiled. Short of such perfect information, security planners must make their best guess of what such a list might look like, using conceptually driven threat analysis to build a model of the terrorist targeting strategy. Planners can then follow the targeting strategy model to evaluate assets from the terrorists' perspective, a technique called "Red Teaming." The planners then build a prioritized target list, based on what choices they would make if they themselves were the terrorists.[210]

The terrorist target list alone does not dictate defensive priorities. It contributes to the overall risk assessment, which considers what the terrorists might do along with what losses the resources owners wish to mitigate. The Red Team's list might accurately assess landfills to be at the top of an environmentalist group's attack list, and the preferred time to attack is late at night. The municipal security planners might consider the electric power plant to be more important to the county's welfare and functioning, though the plant may be low on the terrorists' hit list. The risk assessment suggests an attack at the power plant would be devastating, while a midnight bombing at the dump might would be a mere nuisance. Therefore, it behooves the city to put more effort into shoring up the power plant's security, as opposed to defending the terrorists' prime target, the landfill. Precisely how much effort will depend on where the power plant stands on the terrorists' priority list, and how much risk the city is willing to accept.

The following multi-matrix methodology pulls together the threat and target vulnerabilities into a coherent risk assessment tool that ultimately suggests priorities for antiterrorism planners.

[210] Heymann, pp. 51-52.

Figure 13 depicts a Risk Assessment Matrix.[211] The risk to a target is based on the likelihood, or probability, an attack may occur (on a scale from *unlikely* to *likely*), and the expected loss or damage a successful attack may inflict, also called the severity of an attack (ranging between *minor* to *critical*). The matrix generates a risk score, on a scale of 1 to 5, for an asset (potential target) under consideration, based on the estimated probability and severity of such an attack on that asset.

Risk Assessment Matrix		Attack Probability			
		Likely	Probable	May Occur	Unlikely
Attack Severity	Critical	1	1	2	3
	Serious	1	2	3	4
	Moderate	2	3	4	5
	Minor	3	4	5	5

1 – Critical Risk
2 – High Risk
3 – Medium Risk
4 – Low Risk
5 – Negligible Risk

Figure 13 Risk Assessment Matrix

One uses a series of subordinate matrices to calculate the severity and probability of an attack against a specific target. The Risk Assessment Matrix uses qualitative inputs for an attack's severity (*negligible*, *minor*, *serious* and *critical*) and probability (*unlikely*, *may occur* and *probable*). The subordinate Severity and Probability Matrices generate raw numbers and then translate them to qualitative ratings for the Risk Assessment Matrix.

2. Severity Matrix

The Homeland Security Criticality Assessment Matrix (HLS-CAM) scores the "criticality" of a successful attack based on a number of criteria, each of which is

[211] Adapted and modified from the Marine Corps Institute's Risk Assessment Matrix. See Marine Corps Institute, *ORM 1-0, Operational Risk Management* (Washington, DC: Headquarters Marine Corps, February 2002), pp. 18-19, 38.

examined in its own sub-matrix.[212] (For the purpose of feeding the Risk Assessment Matrix, the term *severity* will substitute for *criticality*, and the HLS-CAM hence will be renamed the *Severity Matrix*.) The sub-matrices quantify a worst-case attack's potential human casualties (deaths and injuries); the economic loss; any effects on critical infrastructure; an attack's symbolic effect; and the environmental impact. A planner uses the sub-matrices (Figure 14) to score these criteria for each potential target, which he then incorporates into the Severity Matrix.

Score	**Death / Injury**
5	Greater than 1,000 deaths or serious injuries
4	100 to 1,000 deaths or serious injuries
3	10 to 100 deaths or serious injuries
2	1 to 10 deaths or serious injuries
1	No deaths or serious injuries

Score	**Economic Impact**
5	Greater than $1 billion in economic loss
4	$100 million to $1 billion in economic loss
3	$10 million to $100 million in economic loss
2	$1 million to $10 million in economic loss
1	Less than $1 million in economic loss

Score	**Critical Infrastructure**
5	Critical long-term vulnerabilities in community infrastructure
4	Critical short-term vulnerabilities in community infrastructure
3	Long-term disruptions to community infrastructure
2	Short-term disruptions to community infrastructure
1	No serious infrastructure impact

Score	**Symbolic Effect**
5	Unique national icon associated with America and recognized internationally
4	Important symbol of America recognized internationally
3	Nationally recognized symbol of America
2	Regionally important symbol
1	Locally important symbol

Score	**Environmental Impact**
5	Complete destruction of multiple aspects of the ecosystem over a large area
4	Complete destruction of multiple aspects of the ecosystem over a small area
3	Long-term serious damage to the ecosystem
2	Short-term serious damage to the ecosystem
1	Small event with minimal, localized, individualized impact on the ecosystem

Figure 14 Severity Sub-Matrices

[212] John C. Rowland, "The New Terrorism: Global Jihad," International Counter-Terrorism Officers [sic] Association 2nd Annual Conference, Las Vegas, NV, lecture, 28 September 2004.

Figure 15 depicts the Severity Matrix tool with sample scores. All assets under consideration fall in the first column, one target per row. The planner puts the sub-matrix (criterion) scores for each target in the same row, under the corresponding criterion column (columns 2 through 6). The scores in a given row are added together to form a total for each target, which becomes the target's *severity score* in column 7. In the event two or more assets tie in *severity score* (like Asset 3 and Asset 4 in Figure 15), their relative *death/injury* values in column 2 break the tie to determine their rank order (*ranking*) in column 8.[213] The *ranking* prioritizes the potential destruction each asset contributes to the overall assessment. The Risk Assessment Matrix uses qualitative labels for the severity, which translate directly from the numerical *severity score*.

Asset	Death/ Injury	Economic	Critical Infrastructure	Symbolic	Environ-mental	Severity Score	Ranking	Risk Assessment Severity
Asset 1	2	4	5	1	1	13	2	Moderate
Asset 2	5	4	4	1	2	16	1	Serious
Asset 3	2	2	2	3	1	10	4	Minor
Asset 4	3	3	1	2	1	10	3	Minor

Severity Score
Point total range: 5-25 points

Severity Score	Risk Assessment Severity
5	Negligible
6-10	Minor
11-15	Moderate
16-20	Serious
21-25	Critical

Figure 15 Severity Matrix (HLS-CAM)

3. Probability Matrix

A Probability Matrix scores the relative likelihood or probability of attack against a field of assets (Figure 16). The Probability Matrix functions much like the Severity Matrix, where assets are compared based on their scores in underlying criteria. Each probability criterion—terrorist targeting method of operations, terrorist capabilities and

[213] All other things being equal, the human casualty toll trumps a tie. If two or more assets remain tied after factoring in the death/injury scores, they should remain tied, as further refinement is unnecessary.

target vulnerability—gets its score from its own respective sub-matrix. Figure 17 illustrates the probability sub-matrices. Once again, each target's final *probability score* in column 5 must be converted to a qualitative *risk assessment probability* in column 6 that will feed the Risk Assessment Matrix.

Asset	Terrorist Targeting MO	Terrorist Capabilities	Target Vulnerability	Probability Score	Risk Assessment Probability
Asset 1	1	2	1	4	Unlikely
Asset 2	3	1	2	6	May Occur
Asset 3	3	3	1	7	Probable
Asset 4	2	2	1	5	May Occur

Mishap Probability Score
Point total range: 3-9 points

Mishap Probability Score	Risk Assessment Probability
3-4	Unlikely
5-6	May Occur
7-8	Probable
9	Likely

Figure 16 Probability Matrix

Score	Terrorist Targeting MO
3	Fits known, demonstrated target preferences and method
2	Fits desired preferences, but never or rarely demonstrated
1	Does not fit preferences

Score	Terrorist Capabilities
3	**Probable:** Easy to accomplish; well within known, demonstrated capabilities
2	**Possible:** Difficult to accomplish; not within demonstrated capabilities
1	**Unlikely:** Extremely difficult; not within estimated capabilities

Score	Target Vulnerability
3	**High:** Easy to penetrate; minimal or non-existent security
2	**Moderate:** Difficult to penetrate; appreciable degree of security
1	**Low:** Extremely difficult to penetrate; high degree of security

Figure 17 Probability Sub-Matrices

The likelihood a target will be attacked stems partly from the terrorists' motive and intent, which a thorough threat assessment should ascertain and feed into the Red Team's targeting strategy model. The planners (or Red Team) consider how a terrorist group might attack a given asset and compare that method to the terrorists' known or suspected capabilities, as well as the group's target preferences. In some cases, a terrorist organization has historically demonstrated a penchant for striking certain targets; in other instances, they have expressed a desire to do so—perhaps issued threats to that effect—but have yet to pull off an attack against such a target. A terrorist group may not have succeeded in attacking a certain target type, but if they've tried in the past, however unsuccessful they may have been, they clearly have shown their intent. (Ahmed Rezzam's attempt to collapse the World Trade Center in 1993 was unsuccessful, but the intent was clear. Al-Qa'eda's successful re-attack in 2001 may have been, in part, an effort to complete unfinished business and to demonstrate Islamist resolve to the United States.)

The terrorists also consider their own capabilities and an asset's vulnerability in selecting targets. Terrorists will strike a target that offers reasonable hope of success. These two planning factors round out the inputs to the Probability Matrix.

4. Cross-Feeding the Matrices

Figure 18 illustrates the entire multi-step risk assessment process. The threat assessment feeds the vulnerability assessment, both of which inform the probability sub-matrices. Meanwhile, threat information concerning the terrorist MO and capabilities allows planners to gauge the potential severity of an attack against each resource, given its current vulnerabilities. The planners generate results from the respective sub-matrices to populate the Severity Matrix and the Probability Matrix, which in turn provide inputs to the final Risk Assessment Matrix. The Risk Assessment Matrix identifies the assets that need priority attention. The planners can then address the extant vulnerabilities of those assets, previously identified in the vulnerability assessment, by devising antiterrorism countermeasures.

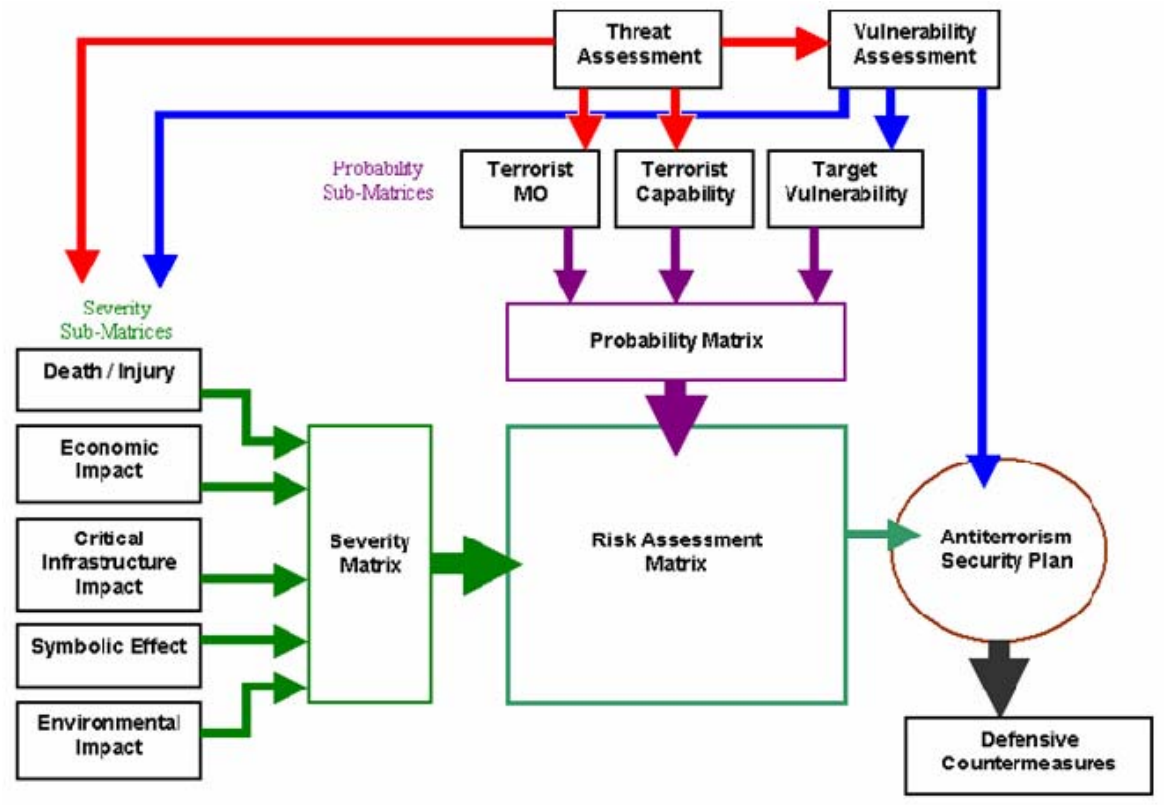

Figure 18 Risk Assessment Process

The Multi-Matrix Method's key strength is that it limits the subjectivity in the decision-making. Granted, planners cannot entirely eliminate subjectivity, particularly in

the early assessment phases, but the multi-matrix method reduces its influence. The tool arithmetically generates risk measures for each asset. The results sometimes prove counterintuitive: the matrix may identify a high-priority asset that planners, based on a simple gut check, had previously considered low-risk. Appendix Y offers an illustrative example of how the Multi-Matrix Method operates.

C. CONCLUSION

Resource protection and security planning, once the purview of local jurisdictions, has become a national endeavor, with the Department of Homeland Security assuming new responsibilities at the federal level. Today, planning and prioritization occur at all echelons, from the local jurisdiction to the federal level. Building uniform planning and prioritization criteria and methods that can be used across the country and at all levels becomes even more important to provide an even level of asset protection and resource allocation.

Antiterrorism planning begins with a good intelligence evaluation of potential threats. Once a broad assessment has identified likely threats and targets (assets), security planners must identify the vulnerabilities of those assets and evaluate the potential risks they face, thereupon selecting the appropriate defensive countermeasures. (Planners must also weigh unintended side-effects that a given security measure may induce, lest they negate the measure's value.)

Security planners have innumerable potential targets to consider, and limited resources with which to defend them. A solid risk assessment prioritizes defensive planning, from which point security specialists figure out how to protect or defend the specific assets. Proper security planning boils down to a cost-benefit analysis of each security countermeasure under consideration. Arithmetic decision matrices take much of the guesswork out of security planning. A multi-layered technique, called the Multi-Matrix Method, feeds intelligence-based threat and vulnerability assessments into decision matrices to compare the risks facing multiple assets.

VI. CONCLUSION

Transnational Islamist terrorism no longer remains the relatively exclusive concern of national intelligence agencies, the military or the Federal Bureau of Investigation. Post-9/11, the American public entrusts every law enforcement organization, from federal to local, to protect the people in its respective jurisdiction. The department or office at each echelon has functions to perform, and all must integrate their efforts to be effective.

Law enforcement officers face a pervasive, religiously motivated threat, that arguably evolved into its modern form on the battlefields of Afghanistan. The campaign against the 1979 Soviet invasion became a political touchstone for the Muslim world, presenting the Muslim community, the *umma*, with an ideal Islamic archetype in the microcosm of a unified jihad. Foreign volunteers of disparate nationalities joined in one common Islamic cause and forged a cohesive tribal loyalty, or *asabiya*, on the battlefield.[214] This laid the foundations of an international network of *mujahed* brethren, who returned to their respective home countries imbued with a spirit of jihad and eager to supplant their oppressive governments with more Islamic regimes. Unfortunately for them, the jihadis lapsed into localism and factionalism, tearing apart the once-unified brotherhood. The movement had lost its jihadi *asabiya* to parochial, nationalist interests.[215] Osama bin Laden endeavored to reinvigorate the jihad in the 1990s by redirecting the jihadis' focus from their domestic regimes—the near enemy—to a more international campaign against the West.[216] He succeeded in achieving a measure of unified action through his al-Qa'eda network, but failed to reconcile divergent interests and eliminate in-fighting.[217] Post-9/11, al-Qa'eda's leaders appear to have adapted a geographically distributed network to a strategic framework that affords local jihadi affiliates a measure of operational leeway, while aligned with the broader goals of the global campaign.

[214] Fawaz A. Gerges, *The Far Enemy: Why Jihad Went Global* (New York, NY: Cambridge University Press, 2005), p. 86.

[215] Ibd., pp. 117-118.

[216] Ibid., pp. 117-118.

[217] For details on the fractures in the jihad, see Gerges, pp. 151-184.

The global jihad network may be distributed and in places decentralized, but law enforcement officers must resist the temptation to apply overly generalized characterizations to the global apparatus. It has become fashionable to paint the entire global jihadi cooperative as a fully decentralized entity, simply by virtue of being a network. Such "net think" potentially shackles and biases the analysis of the terrorist apparatus, blinding officials to the subtleties of a network's structure that may be susceptible to manipulation. Certain elements, such as al-Qa'eda's High Command, still retain a hierarchical structure; al-Qa'eda continues to exert as much control as it can over worldwide operations through direct instruction, by means of training and resource control, or through ideologues who frame jihadi discourse and encourage compliance with al-Qa'eda's strategic and tactical preferences. Grand ideology guides the terrorists' strategy, which in turn directs the operational tactics and methods. The Internet bridges and blends the strategic and tactical levels of operation, and fosters communication in an environment of relative security. An unbiased analysis of the jihadi network requires officials to delve into terrorist rhetoric, strategy and operational communications, most of which can be gleaned from the Internet—if they know where to search. Examining the substance of network internodal linkages—primarily communications content—analysts can flesh out any hierarchical command relationships. From there, officials can tactically isolate key power players to hinder jihadi communications and their command and control mechanisms; they may interdict resource flows in order to hobble terrorist operations or to flush out previously unknown organizational redundancies and network members.

Officials charged with antiterrorism planning should remain leery of network-on-network solutions that paint the global jihad as a fully decentralized, nearly leaderless enterprise that must be counteracted with equally decentralized operations. Eschewing vertical operational management risks sacrificing strategic insight and synchronization for tactical innovation, predicated on the erroneous presumption that hierarchical counteraction strategies are inherently viscous and unresponsive. Centrally managed antiterrorism and counterterrorism strategies, particularly those concerning intelligence exploitation, may prove more effective at recognizing faults or weaknesses that law enforcement agencies can exploit in proactive operations.

Cleavages persist in the jihadi enterprise to this day. They reveal both potential targets and allies in the fight against Islamist terrorists. Some outlying associates in the network have looser loyalties to the global jihad, and law enforcement operations may pick them off, culling them from the larger network. Law enforcement agencies may neutralize these weak nodes either through arrests or by co-opting them as cooperating assets. Additionally, rivalries between factions or individuals within the network may represent leverage points that can be exploited; competitors in the jihadi enterprise may be pitted against each other, either as recruited informants or unwitting assets.

Human intelligence is the key to collecting on the Islamist terrorist threat. Human sources of information provide insight into the secretive world of the clandestine jihadi apparatus, offering clues that technical intelligence platforms are ill-suited to detect. Additionally, while they may lack the technical collection systems that national intelligence agencies possess, law enforcement agencies boast a long tradition of employing human informants and therefore have a strong baseline in sourcing. Ethnic and religious demographics make the process somewhat tricky, but proper cultural understanding will help law enforcement officers partner with suitable members of society to target their collections. From imams to *mukhtars*, the Muslim community presents a number of knowledgeable members who can serve as signposts or active participants in the campaign to identify and eliminate jihadi operatives in their midst.

Analysis is crucial. Historical and recent intelligence failures can be traced to poor or non-existent analysis. Police generally lack the resources or institutional background to field an effective and broad antiterrorism analytical capability. However, a multi-layered approach seems to offer the best means of bringing local intelligence to higher echelons, and to capitalize on regional and national analytical organs to build a cooperative that can detect and challenge geographically dispersed patterns of terrorist activity. A cooperative analysis network that integrates both vertical and horizontal relationships may prove the most effective.

Finished, analyzed intelligence represents the currency of defensive planning and terrorism countermeasures. Sound threat and vulnerability assessments, rooted in good intelligence, allow planners to identify likely terrorist targets, evaluate the risks the

targets face, and prioritize protective resources. Efforts by the Department of Homeland Security to manage asset prioritization nation-wide revealed stark inconsistencies and subjectivity in state and local risk evaluations. This highlights the need for a common risk assessment strategy. The Multi-Matrix Method proposed in this thesis, if applied at all echelons, may increase risk assessment objectivity and help bring the country to a common standard.

The global jihad is purposefully secretive and elusive, and the targets they have to choose from are countless. Sound intelligence empowers law enforcement professionals to get ahead of terrorist targeting, to prevent future attacks and to weaken the Islamist terrorist network in America. Armed with intelligence tools, law enforcement officers will be effectively policing toward a de-clawed jihad.

APPENDIX A. AL-QA'EDA INTELLIGENCE REQUIREMENTS[218]

A. FOR TARGETING AN INDIVIDUAL PERSON[219]

- Biographical information (name, age, marital status, whether he is armed)
- Residential information (home address, entrances and exits, neighborhood characteristics, means to enter covertly, armed security on premises)
- Type of employment
- Commute times between home and work
- Commuting routes between home and work
- Information on his car
- Names and addresses of his friends
- Leisure activities or hobbies, known vacation spots
- Information on stores he may frequent
- Information on spouse's employment
- Information on the children's school and whether target ever visits the school
- Mistress or girlfriend, address and times he visits her
- Information on his doctor

B. FOR TARGETING A FACILITY OR ACTIVITY

- Specific location
- Exterior shape of the facility
- Area or acreage of facility
- Number of rooms and floors inside any buildings
- Number of occupants
- Telephone line information, including switchboard location
- Information on other means of communication
- Electric power access

[218] *Military Studies in the Jihad against the Tyrants* [a.k.a. *The al-Qa'eda Terrorist Training Manual* or *The Encyclopedia of Jihad*], [attributed to Al-Qa'eda, ca. 1992 or 1993, translated by the Greater Manchester Constabulary, UK, ca. 2002], pp. UK/BM-72-73, 90-91.

[219] The manual is worded specifically for a target of male gender.

- Parking
- Information on vehicles in the facility
- Lighting (location, brightness, timing)
- Security (guards, locations, types of weapons and ammunition on site, response protocols, fortifications and any tunnels)
- Command structure with biographical information of high-ranking personnel
- Names of units or organizations assigned to the facility
- Leave or liberty policy
- Shift schedules (sleeping and waking periods)
- Physical layout and environment (urban, rural, dense or open space)
- Neighborhood characteristics and socioeconomic environment
- Any public parks in vicinity
- Nearby government or police offices, including diplomatic establishments
- Width and direction of travel for roadways in the vicinity
- Traffic information (times of heavy congestion, traffic signal information, pedestrian areas, types of transportation that afford access to the location)

APPENDIX B. EXAMPLE SOURCE OPERATIONS[220]

Potential Source: Taxi Service Dispatch Manager		
Source Type: Open Contact[221]	**Source Access:** Proximal Outsider or Detached Associate	**Source Placement:** Resource-Specific[222] or Suspect-Specific
Information Type: Drivers, shift schedules, fare earnings		
Reportable Indicators	**Significance**	

[220] Mariani lists numerous potential sources with resource-specific or target-specific access. See Cliff Mariani, *Terrorism Prevention and Response: The Definitive Law Enforcement Guide to Prepare for Terrorist Activity*, 2nd Edition (New York, NY: Looseleaf Law Publications, Inc., 2004), pp. 128-132.

[221] Generally, a source repeatedly reporting on a specific individual suspect may expect to face a greater degree of risk than the occasional reporter. In such a case, he should be treated as a confidential informant, rather than an open contact.

[222] Resource-Specific, in the context of employment, simply means that specific type of work or employment with the company provides a mechanism by which a terrorist operative may gain access to material or targets. The resource in this context is the employment itself, or the position with the company.

Driver repeatedly volunteers to fill in on others' shifts. Driver repeatedly works extra shifts Driver repeatedly changes or requests to change his shift (day to night, night to swings, etc.).	Driver may be trying to get exposure to traffic patterns at different times of day in effort case traffic around a target (traffic representing potential attack victims or traffic representing a planning factor for access to and escape from the target, i.e. ingress and egress routes).
Driver's fare earnings are uncharacteristically low for hours worked. Driver calls in off-duty while out on the road, or spends a lot of time in the car off the clock.	Driver may be using his job as taxi driver as cover to case targets, access and escape routes, and traffic patterns, as above. Excessive time off the clock suggests the driver may be driving without taking fares, leaving himself the initiative to drive where and when he wants; passengers (fares) force the driver to adhere to someone else's agenda.
Driver may display jihadi paraphernalia in his taxi.	Jihadi paraphernalia may indicate sympathy or support for terrorist causes.

Potential Source: Construction Foreman or Day Labor Foreman		
Source Type: Open Contact	**Source Access:** Proximal Outsider or Detached Associate	**Source Placement:** Resource-Specific or Target-Specific; may evolve into Suspect-Specific
Information Type: Laborers, job site preferences, laborer skill levels, laborer inquiries		

Reportable Indicators	**Significance**
Prospective worker expresses interest in working on specific job sites connected to potential targets in critical infrastructure or key assets; job sites may be at or near the targets, to include sites giving clear view of a given target. If a day laborer passes up a job offer because the job site doesn't match his specific criteria, this is a bigger clue.	Prospective laborer may be a scout, seeking access to surveil (observe over time) or reconnoitre (make a one-time observation to acquire specific details about) a target.
Laborer demonstrates low skill level on the job.	Prospective laborer may not have the requisite experience for the task and may be simply using the employment as a ruse to gain access to a target or materials.

Worker may ask detailed questions about the target, with particular attention to vulnerabilities or means to gain future access. Worker may spend inordinate amount of time observing or studying the target, rather than focusing on the job. May take notes or photographs. Worker attempts to gain employment with demolition crew without proper background or bona fides; worker on construction team may try to gain access to demolition crew and materials.	Prospective laborer may be using the employment to collect pre-attack intelligence on a potential target (target casing). Prospective laborer may be attempting to gain access to demolition materials and equipment, which he may divert to a terrorist cell.

Potential Source: Utilities Service Supervisor or Meter Reader		
Source Type: Open Contact	**Source Access:** Unaffiliated Observer	**Source Placement:** Suspect-Specific
Information Type: Utilities consumption		

Reportable Indicators	**Significance**
Unusual utilities consumption patterns.	May point to production of chemical or biological weapons. (Not exclusive to terrorist weapons production--may also be indicative of illicit drug production.)

Potential Source: **Landlord or Apartment Superintendent**		
Source Type: Open Contact or Confidential Informant (Confidential Informant if risk is posed by routinely informing on tenants)	**Source Access:** Detached Associate	**Source Placement:** Suspect-Specific
Information Type: Tenant activities and living conditions		

Reportable Indicators	**Significance**
Multiple male residents in a single apartment, apparently secretive.	May indicate the presence of a clique or cell. (Multiple roommates should not be the sole indicator; however, secretive behavior suggests the group may have something illicit they wish to hide.)
Unusual living conditions observed during service calls, such as a lack of furnishings but the presence of medical supplies or chemistry equipment and industrial chemicals; potted plants or hydroponics; video or photography equipment, maps, diagrams, schematics and blueprints; multiple respirators or gas masks; multiple itineraries or schedules; or computer equipment.	The apartment may appear to be more of an operational staging area or safehouse, rather than a long-term residence. Presence of operational items may point to pre-operational planning, weapons acquisition or even weapons development (including small-scale chemical or biological weapons).

Potential Source: **Halal Grocer**		
Source Type: Open Contact	**Source Access:** Detached Associate	**Source Placement:** Resource-Specific or Suspect-Specific
Information Type: Patron information		

Reportable Indicators	**Significance**
Observation of any patrons who might appear radicalized or Salafi. May harass other customers for not being pious enough, or may praise them for shopping in a Halal store.	Points to the presence of radicalized Salafist cliques.

Potential Source: **Halal Grocery Patron**		
Source Type: Open Contact	**Source Access:** Proximal Outsider	**Source Placement:** Resource-Specific or Suspect-Specific
Information Type: Information on other patrons, information on the store proprietors, direct observation of any jihadi paraphernalia in the store		

Reportable Indicators	**Significance**
Observation of any patrons who might appear radicalized or Salafi. May be harassed by radical Salfist customers for not being pious enough, or may be praised by them for shopping in a Halal store.	Points to the presence of radicalized Salafist cliques.
Presence of any jihadi paraphernalia in the store, such as pro-jihadi posters, photos, shrines, posters or calendars honoring suicide bombers.	Suggests a pro-jihad leaning on the part of the Halal proprietor.[223]

[223] Gerald Posner, *Why America Slept: The Failure to Prevent 9/11* (New York, NY: Random House, 2003), p. 3; First Technologies, LLC., "Understanding Islamist Militant Terrorism and Prevention Strategies," Federal Law Enforcement Training Center, Glynco, GA, 16-17 September 2004.

Potential Source: ***Mukhtar*** **(Neighborhood Leader)**		
Source Type: Open Contact	**Source Access:** Detached Associate	**Source Placement:** Resource-Specific[224] or Suspect-Specific
Information Type: Neighborhood member information, neighborhood activities, signs of radical newcomers or emergent radical elements		

Reportable Indicators	**Significance**
Emergence or arrival of vocal, radical elements; emergence of Salafist cliques; scheduled visits in the area by outspoken, radical speakers or imams; approaches by people raising funds for suspect charities or jihadi causes; indications of individuals or small groups seeking inroads to the Global Jihad; changes in neighbor behavior indicative resulting in significant shift in political or religious views, or noticeable change in an individual's circle of friends (particularly cases of withdrawal from one's immediate family).	The emergence of radical elements may suggest the early formation of pro-jihadi or actual jihadi cliques, or possibly even terrorist cells. Changes in individuals' associations and social habits may also suggest newfound membership in such a clique.

[224] In this context, *mukhtar*'s community services or the community's general support structure constitute the resource.

Potential Source: **Mosque Imam**		
Source Type: Open Contact or Confidential Informant	**Source Access:** Detached Associate	**Source Placement:** Resource-Specific[225] or Suspect-Specific
Information Type: Mosque congregant information, community activities, signs of radical newcomers or emergent radical elements, identification of radical imams at other mosques, identification of radical speakers on presentation circuits		

Reportable Indicators	**Significance**
Emergence or arrival of vocal, radical elements; emergence of Salafist cliques; scheduled visits in the area by outspoken, radical speakers or imams; approaches by people raising funds for suspect charities or jihadi causes; indications of individuals or small groups seeking inroads to the Global Jihad; changes in a congregant's behavior indicative resulting in significant shift in political or religious views (such as increased piety or devoutness), or noticeable change in an individual's circle of friends.	The emergence of radical elements may suggest the earlier formation of pro-jihadi or actual jihadi cliques, or possibly even terrorist cells. Individual shifts in piety may point to a growing Salafi influence in the congregation. Changes in individuals' associations and social habits may also suggest newfound membership in a Salafi clique.

[225] In this context, the resource is the mosque, religious services or religious ministry.

Potential Source: **Mosque Congregant**		
Source Type: Open Contact	**Source Access:** Unaffiliated Observer or Proximal Outsider	**Source Placement:** Resource-Specific or Suspect-Specific
Information Type: Information on activity in the congregation, information on the clergy's views and activities		

Reportable Indicators	**Significance**
Emergence or arrival of vocal, radical elements; emergence of Salafist cliques; scheduled visits in the area by outspoken, radical speakers or imams; appeals by people raising funds for suspect charities or jihadi causes; indications of individuals or small groups seeking inroads to the Global Jihad; changes in a congregant's behavior indicative resulting in significant shift in political or religious views (such as increased piety or devoutness), or noticeable change in an individual's circle of friends.	The emergence of radical elements may suggest the earlier formation of pro-jihadi or actual jihadi cliques, or possibly even terrorist cells. Individual shifts in piety may point to a growing Salafi influence in the congregation. Changes in individuals' associations and social habits may also suggest newfound membership in a Salafi clique.
Noticeable radicalism in the mosque clergy, or the arrival of new imams with pro-jihadi views.	Radicalism in the clergy may incline the mosque and congregation to support jihadi causes and operatives.
Power struggles in the mosque between moderates and radicals.	In-fighting among the clergy may point to external elements attempting to usurp the mosque to use as a jihadi base.[226]

[226] This is what happened at the Alkifah Center in Brooklyn, when the blind sheikh, Omar Abdel Rahman precipitated a radical takeover after his arrival in 1990. See Posner, pp. 7-10.

Potential Source: Medical Supplier, Scientific Equipment Supplier, or Brewing Equipment Supplier		
Source Type: Open Contact	**Source Access:** Unaffiliated Observer	Source Placement: Resource-Specific
Information Type: Equipment and material sales, customer information		

Reportable Indicators	**Significance**
Destination for medical or scientific equipment is not an educational or scientific institution, but a private residence or post office box. An apparently devout Muslim (particularly one dressed and groomed in Salafi manner) purchasing beer-brewing supplies would be incongruous.	The purchase may be for distillation of weaponized chemical or biological agents.

Potential Source: **Pharmacist**		
Source Type: Open Contact or Confidential Informant (Confidential Informant if used in a sting operation)	**Source Access:** Proximal Outsider	**Source Placement:** Suspect-Specific
Information Type: Unusual prescription activity		

Reportable Indicators	**Significance**
Suspect filling prescriptions for large quantities of powerful antibiotics. Prescription may be written by an out-of-town physician, an apparently foreign or immigrant physician, or physician new to the area. Note: Suspect may fill multiple, small-quantity prescriptions at different pharmacies to avoid detection. Detection of such "pharmacy shopping" requires sourcing multiple area pharmacists.	Suspect may be working on culturing biological agents or biotoxins.

Potential Source: Transportation System Employees (Token Booth Attendants, Flight Attendants, etc.)		
Source Type: Open Contact	**Source Access:** Unaffiliated Observer	**Source Placement:** Target-Specific
Information Type: Visitor and commuter behavior		

Reportable Indicators	**Significance**
Photographing or videotaping entryways and exits; security measures and personnel; crowds and traffic patterns. Emphasis on capturing signs identifying a station or a particular office is noteworthy.	May be a target casing. Taking special note of distinct markings or signs that identify the asset suggests an attempt to highlight the means by which a subsequent planning team or attack team may recognize the specific target.

Potential Source: **Employees at Significant Tourist Landmarks**		
Source Type: Open Contact	**Source Access:** Unaffiliated Observer	**Source Placement:** Target-Specific
Information Type: Visitor and patron behavior		

Reportable Indicators	**Significance**
Patron expresses interest in blueprints, architectural designs, or structural data for the facility. Photographing or videotaping entryways and exits; security measures and personnel; crowds and traffic patterns.	May be an attempt to case the facility for an attack, with designs on finding access points and structural vulnerabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. AUTOMATIC ANALYTICS: FROM FIELD REPORT TO DATABASE

A patrolman cited a driver and passenger for littering on Tuesday. She observed the subjects pull up to the curb in front of the federal courthouse at 4:06 p.m., toss a brown paper bag from the passenger window onto the courthouse steps, and drive away. The officer pulled them over at the end of the block and issued a ticket for littering. She also went back to retrieve the paper bag, which contained a wad of modeling clay weighing approximately three pounds.

The officer's report lists the subjects' names, passport information, the name of the hotel where they are staying, and pertinent rental car information. It also includes the time and location of the incident with a brief synopsis.

An analyst then processes the field report for entry into the automated database. He feeds different data fields in the system drawn from the information the officer recorded during the traffic stop. The analyst must also apply some of his own training and interpret the event. Was it a simple littering offense? Did the time and location have some significance? Perhaps federal court cases recess around 4 p.m.—about the time of this incident. Three pounds of modeling clay is an odd thing to toss out of a car window; an empty fast food bag or Styrofoam coffee cup would be more common. This anomalous behavior, combined with the location, suggests to the analyst this might be a dry run, or rehearsal, for a possible hand-tossed explosive device attack.

The analyst must select the appropriate activity categories in the database, such as *rehearsal*. All the other data go into the appropriate data fields. Once the analyst has entered all the available data, the system can begin the automated analytic evaluation.

The system should ideally cross-reference multiple databases to find connections to the data elements in the police analytic database. This process identifies another individual from the same country who rented a car from the same rental agency and stayed in the same hotel one month earlier. Though his name isn't in the police analytic database (having not been cited for any offense), cross-referencing hotel and rental car databases turned up his name. Federal court dockets list a terrorism indictment hearing

scheduled at that courthouse on a Tuesday next month. A captured terrorist suspect happens to be the government's prime witness.

The computerized analytic system may note the commonalities, whereupon the analyst can recommend a collection plan for further intelligence gathering. Police may stake out the area around the courthouse to observe pre-operational surveillance or dry run activity. Over the next month, their observations help the analyst feed the database with vehicle descriptions, license plate numbers, incident times and activity details. The system crunches the data and shows a pattern of similar activity on various days of the week around 4 p.m., with increasing frequency as the court date gets closer—and there is at least one apparent dry run every Tuesday. The predictive result is that an attack is possible against people exiting the courthouse following the terrorism indictment hearing, perhaps more specifically against the terrorist who turned state's evidence.

APPENDIX D. MULTI-MATRIX METHOD: EXAMPLE ASSESSMENT

A hypothetical example of the multi-matrix risk assessment method follows.

Step 1: Build Terrorist Attack Strategy Model

The security planners practice Red Teaming to build a terrorist targeting strategy model for al-Qa'eda and its affiliates. They glean intelligence reports and consult analysts to devise the model, which gives them their baseline planning assumptions.

Primary Terrorist Threat - The primary terrorist threat of concern is from transnational Islamist terrorists affiliated with the Global Jihad, namely al-Qa'eda and its affiliates.

Predominant Transnational Islamist Terrorist Method of Operations (MO) –

- Plan mass casualty attacks
  - Mass gatherings at special events
  - Tourist attractions (e.g., Bali, Indonesia bombing in 2002 and 2005; Jordan plots in 1999; Sharm El-Sheikh, Egypt bombings in 2005)
  - Hotels - popular target based on current trend in East Asia (e.g., Jakarta, Indonesia bombing 2003) the Middle East and Africa (e.g., Amman, Jordan plot in 1999 and attacks in 2005; Mombassa, Kenya attack in 2002; attack in Casablanca, Morocco in 2003; bombings in Taba and Sharm El-Sheikh, Egypt in 2004 and 2005 respectively)
  - Mass transit (e.g., Madrid, Spain train bombing in 2004, London, U.K. metro and bus attacks in 2005[227])

[227] Al-Qa'eda's affiliation with the cells that perpetrated the Madrid and London attacks remains a matter of debate, as the financial, operational and inspirational links have not been firmly established. Whether the groups acted on behalf of al-Qa'eda, or merely followed al-Qa'eda's jihadi model, the resultant attacks did fit the mass casualty and multi-target paradigm.

- Conduct simultaneous attacks against multiple targets[228] (e.g., U.S. embassies in Africa, 1998; 11 September, 2001; Madrid and London rail attacks) Note: This is only a partially a relevant factor in local analysis, since the multiple attacks can be separated over great geographic distances for effect, rather than concentrating as multiple attacks within one locality. A centrally directed al-Qa'eda operation may attack targets in different states or different countries, while an affiliated grass-roots jihadi cell may only be capable of striking multiple targets within the same city.
- Prefer perceived hard targets (embassies, military assets overseas), but trend toward soft, high-profile targets (e.g., U.S. embassies in Africa were more vulnerable than diplomatic facilities in more dangerous countries;[229] The USS Cole and USS The Sullivans were transiting, not moored in a naval port)
- Prefer vehicle-borne explosive devices, such as trucks, boats or aircraft (e.g., U.S. embassies in Africa; Bali in 2002 and 2005; 2000 attempt on the USS The Sullivans and attack on the USS Cole in Aden, Yemen; 11 September 2001.)
- Expressed desire for weapons of mass destruction, but no successful attacks to date (some plans have been foiled or interdicted)[230]
- Expressed desire for economic impact,[231] though rarely the primary focus of attack

Step 2: List Assets to Protect

Next, the planners compile a list of assets they wish to protect from terrorist attack:

- Grand Hotel on the Boardwalk
- Subway Train System
- Nuclear Power Plant
- Public Library

[228] Bruce Teft, "Terrorism Awareness—Islamic Terrorism: Origins and Prevention," International Counter-Terrorism Officers [sic] Association 3rd Annual Conference, Orlando, FL, lecture, 18 October 2005.

[229] "FBI leads bombing investigation; security warnings reviewed," *CNN.com*, 13 August 1998, http://www.cnn.com/WORLD/africa/9808/13/embassy.fbi.03/ (accessed 21 May 2006).

[230] Teft.

[231] Teft, citing bin Laden's 29 October 2001 statement on the 9/11 attacks.

Step 3: Calculate Severity of Terrorist Events

The planners assume a high-explosive device as the preferred method to maximize carnage (as derived from the attack model). Specifically, they surmise the attack on the Grand Hotel would take the form of a truck bomb (worst case). They postulate a subway attack would consist of multiple backpack charges placed by pedestrian terrorists, or explosive vests detonated by suicide bombers. The most effective means to get an explosive onto the nuclear power plant would be by means of a small, explosive-laden aircraft. Finally, they hypothesize either a vehicle bomb outside the building, or pedestrian bombers inside, would be the most effective means to attack the public library. The planners then rate each potential target against each criterion in the severity sub-matrices (Figure 19). They note those values in the Severity Matrix (Figure 20).

Asset	Death/ Injury	Economic	Critical Infrastructure	Symbolic	Environmental
Grand Hotel	Several hundred	$50-75 million	No serious impact	Regional symbol	Minor, localized impact
Subway	200-500	$25-50 million	Critical, long-term with ripple effects on remaining transportation infrastructure	Local symbol	Minor, localized impact
Nuclear Power Plant	1000*	$100-150** million	Critical long-term vulnerabilities in community infrastructure (electric power grid)	Local symbol	Complete destruction of multiple aspects of the ecosystem over a small area
Library	Between 10 and 100	$15 million	No serious impact	Local symbol	Minor, localized impact

*Estimate 200 dead and up to 1000 sick from radiation poisoning.
**Includes direct facility damages, lost revenue, costs to purchase electricity from other sources and radiological clean-up costs.

Figure 19 Example Damage Estimates for Each Asset

Asset	Death/ Injury	Economic	Critical Infrastructure	Symbolic	Environ-mental	Severity Score	Ranking	Risk Assessment Severity
Grand Hotel	4	3	1	2	1	11	3	Moderate
Subway	4	3	5	1	1	14	2	Moderate
Nuclear Power Plant	5	5	5	1	4	20	1	Serious
Library	2	2	1	1	1	7	4	Minor

5 → Negligible 11-15 → Moderate 16-20 → Serious
6-10 → Minor 21-25 → Critical

Figure 20 Example Severity Matrix Calculation

Step 4: Calculate Probability of Attack

The planners evaluate an attack against each asset in light of the terrorist MO, terrorist capabilities, and the asset's vulnerabilities to the anticipated form of attack (see Figure 21). All assets are then compared and scored using the Probability Matrix in Figure 22.

Asset	Terrorist Targeting MO	Terrorist Capabilities	Target Vulnerability
Grand Hotel	Fits known, demonstrated target preferences and method	Probable: Easy to accomplish; well within known, demonstrated capabilities	Moderate: Difficult to penetrate; appreciable degree of security
Subway	Fits known, demonstrated target preferences and method	Probable: Easy to accomplish; well within known, demonstrated capabilities	High: Easy to penetrate; minimal or non-existent security
Nuclear Power Plant	Fits desired preferences, but never or rarely demonstrated	Probable: Easy to accomplish; well within known, demonstrated capabilities	Low*: Extremely difficult to penetrate; high degree of security
Library	Does not fit preferences	Probable: Easy to accomplish; well within known, demonstrated capabilities	High: Easy to penetrate; minimal or non-existent security

*The heavy concrete construction makes the nuclear power plant relatively invulnerable to a small aircraft collision.

Figure 21 Example Vulnerability Sub-Matrix Estimates for Each Asset

Asset	Terrorist Targeting MO	Terrorist Capabilities	Target Vulnerability	Probability Score	Risk Assessment Probability
Grand Hotel	3	3	2	8	Probable
Subway	3	3	3	9	Likely
Nuclear Power Plant	2	3	1	6	May Occur
Library	1	3	3	7	Probable

3-4 → Unlikely 5-6 → May Occur 7-8 → Probable 9 → Likely

Figure 22 Example Probability Matrix Calculation

Step 5: Calculate Risk

The planners' final step entails inputting the Severity Matrix and Probability Matrix results into the Risk Assessment Matrix for each asset in turn. (See Figure 23.) The tool generates a risk assessment for each asset relative to the others.

Risk Assessment Matrix		Attack Probability			
		Likely	Probable	May Occur	Unlikely
Attack Severity	Critical	1	1	2	3
	Serious	1	2	3	4
	Moderate	2	3	4	5
	Minor	3	4	5	5

1 – Critical Risk
2 – High Risk
3 – Medium Risk
4 – Low Risk
5 – Negligible Risk

Grand Hotel: Severity = *Moderate*, Probability = *Probable* → Risk = 3 (Medium)

Subway: Severity = *Moderate*, Probability = *Probable* → Risk = 3 (Medium)

Power Plant: Severity = *Serious*, Probability = *May Occur* → Risk = 3 (Medium)

Library: Severity = *Minor*, Probability = *Probable* → Risk = 4 (Low)

Figure 23 Example Risk Assessment Matrix Calculation

The Multi-Matrix Methodology produces a three-way tie between the Grand Hotel, subway and power plant for risk. Planner may break the tie based on relative severity rankings or probability rankings. The hotel and subway are more likely to be struck than the power plant, though the resultant severity of an attack on the power plant brings the risk on par with the other two targets. If planner elects to harden targets based on the likelihood they will be attacked, they would do well to fortify the hotel first, then the subway. If they choose to prioritize the three targets based on the consequences of an attack, then they should harden the power plant.

LIST OF REFERENCES

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, authorized Edition [paperback]. New York, NY: W.W. Norton & Company, Inc., [2004].

Anderson, John Ward and Karen DeYoung. "Plot to Bomb U.S.-Bound Jets Is Foiled: Britain Arrests 24 Suspected Conspirators." *Washington Post Foreign Service* (11 August 2006). http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html?referrer=email (accessed 3 October 2006).

Anonymous. "Understanding Islamist Militant Terrorism and Prevention Strategies." First Technologies, LLC., Federal Law Enforcement Training Center, Glynco, GA. Training Seminar, 16-17 September 2004 and 30 November 2004.

Anonymous. *A Law Enforcement Guide to Understanding Islamist Terrorism*. Baton Rouge, LA: First Capital Technologies, LLC., 2003.

Arquilla, John, and David Ronfeldt. "The Underside of Netwar." *Review – Institute of Public Affairs* (December 2002): 3-5.

Arquilla, John, and David Ronfeldt. "Networks, Netwars, and the Fight for the Future." *First Monday*, vol. 6, no. 10 (September 2001). http://www.firstmonday.org/issues/issue6_10/ronfeldt/ (accessed 19 May 2006).

Arquilla, John, and David Ronfeldt. "The Advent of Netwar (Revisited)." In *Networks and Netwar: The Future of Terror, Crime and Militancy*, edited by John Arquilla John and David Ronfeldt, 1-27. Santa Monica, CA: RAND, 2001.

Autera, Joseph. "Before It Makes the Headlines: Effective Threat Detection Strategies and Tactics." *Journal of Counterterrorism and Homeland Security Studies* (Fall 2003): 36-43.

Beech, Michael F., LTC, U.S. Army. "Observing al Qaeda through the Lens of Complexity Theory: Recommendations for the National Strategy to Defeat Terrorism." [*U.S. Army War College Center for Strategic Leadership*] *Student Issue Paper*, vol. 204-01 (July 2004).

Bergen, Peter L. *Holy War, Inc.: Inside the Secret World of Osama bin Laden*, First Touchstone Edition. New York, NY: Touchstone (Simon & Schuster, Inc.), 2002.

Bermudez, Joseph S., Jr. *Terrorism: the North Korean Connection*. New York, NY: Crane Russack (Taylor & Francis New York, Inc.), 1990.

Bin Laden, Osama. Statement on the 9/11 attacks. Cited by Teft, Bruce. "Terrorism Awareness—Islamic Terrorism: Origins and Prevention." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Bodrero, D. Douglas. "Law Enforcement's Challenge to Investigate, Interdict, and Prevent Terrorism." *The Police Chief* (February 2002): 41-48.

Bolz, Frank Jr.; Dudonis, Kenneth J.; and Schulz, David P. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. Boca Raton, FL: CRC Press LLC, 2002.

Borgatti, Stephen P., Kathleen M. Carley and David Krackhardt. *On the Robustness of Centrality Measures under Conditions of Imperfect Data*. Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d. http://www.analytictech.com/borgatti/papers/robustness.pdf (accessed 6 June 2006).

Brachman, Jarret M. and William F. McCants. *Stealing Al-Qaida's Playbook*. West Point, NY: Combating Terrorism Center, February 2006.

Burke, Jason. *Al-Qaeda: The True Story of Radical Islam*. New York, NY: I.B. Tauris & Co. Ltd., 2004.

Burton, Fred. "Al Qaeda in 2006: Devolution and Adaptation." *STRATFOR* (Strategic Forecasting, Inc.), 3 January 2006. http://www.stratfor.com/products/premium/print.php?storyId=260353 (accessed 18 February 2006).

Burton, Fred. "Al Qaeda: Targeting Guidance and Timing." *Stratfor*, 9 December 2005. http://www.stratfor.com/products/premium/read_article.php?id=259453 (accessed 18 February 2006).

Burton, Fred. "Beware of 'Kramer': Tradecraft and the New Jihadists." *STRATFOR* (Strategic Forecasting, Inc.), 18 January 2006. http://www.stratfor.com/products/premium/read_article.php?id=261022 (accessed 16 February 2006).

Burton, Fred. "The Psychological Battlefield." *STRATFOR* (Strategic Forecasting, Inc.), 10 August 2005. http://www.stratfor.com/products/premium/read_article.php?id=253467 (accessed 18 February 2006).

Cainkar, Louise. "Post 9/11 Domestic Policies Affecting U.S. Arabs and Muslims: A Brief Review." *Comparative Studies of South Asia, Africa and the Middle East*, 24:1 (2004): 245-248. http://muse.jhu.edu/demo/comparative_studies_of_south_asia_africa_and_the_middle_east/v024/24.1cainkar02.pdf (accessed 17 February 2006).

Carley, Kathleen M. *Estimating Vulnerabilities in Large Covert Networks*. Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d. http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/249.pdf (accessed 6 June 2006).

Center for International Issues Research. "Al-Qaida's Global Strategy Part 1 of 5: Antecedents and Evolution." *Global Issues Report* (30 August 2006) [electronic document].

Center for International Issues Research. "Al-Qaida's Global Strategy Part 3 of 5: Phase 2 'Opening the Eyes' Implementation." *Global Issues Report* (6 October 2006) [electronic document].

Center for International Issues Research. "Al-Qaida's Global Strategy Part 4 of 5: Planning for the Future—Phases Four to Seven." *Global Issues Report* (6 October 2006) [electronic document].

Center for International Issues Research. "Al-Qaida's Global Strategy Part 5 of 5: Comparison of Al-Qaida's Seven-Phase Strategy with 'The Management of Savagery.'" *Global Issues Report* (30 August 2006) [electronic document].

Center for International Issues Research. "Postings Cite U.S. 'Economic Weakness,' Call for 'Economic Jihad.'" *Global Issues Report* (27 September 2006) [electronic document].

Chechen Jihadi Documentation Video. http://www.ogrish.com/archives/footage_of_car_bomb_blowing_up_near_army_convoy_chechnya_2001_Sep_12_2004.html (accessed 5 November 2006).

Coll, Steve and Glasser, Susan B. "e-QAEDA: From Afghanistan to the Internet—Terrorists Turn to Web as Base of Operations." *The Washington Post*, Sunday, 7 August 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (accessed 4 November 2006).

Combating Terrorism Center. *Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities*. West Point, NY: Combating Terrorism Center, 14 February 2006.

Conway, Maura. "Terrorism and IT: Cyberterrorism and Terrorist Organizations Online." In *Terrorism and Counterterrorism: Understanding the New Security Environment*, eds. Russell D. Howard and Reid L. Sawyer. Guilford, CT: McGraw-Hill/Dushkin, 2004.

Cullison, Alan. "Inside Al-Qaeda's Hard Drive." *The Atlantic Monthly* (September 2004). http://www.theatlantic.com/doc/200409/cullison (accessed 3 November 2006).

Davis, Paul K. and Brian Michael Jenkins. *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda*. Santa Monica, CA: RAND National Defense Research Institute, 2002.

Defeating the Jihadists: A Blueprint for Action. Century Foundation Task Force. Richard A. Clarke, chairman. New York, NY: The Century Foundation Press, 2004.

Dowling, Thomas. "Failures of Imagination: Thoughts on the 9/11 Commission Report." *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 7-16.

Eldridge, Thomas R.; Ginsburg, Susan; Hempel, Walter T. II; Kephart, Janice L.; and Moore, Kelly. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: 2004. (Electronic version.)

"FBI leads bombing investigation; security warnings reviewed." *CNN.com*, 13 August 1998. http://www.cnn.com/WORLD/africa/9808/13/embassy.fbi.03/ (accessed 21 May 2006).

Federal Bureau of Investigation. "Most Wanted Terrorists." [Official government web site.] http://www.fbi.gov/wanted/terrorists/teraladel.htm (accessed 3 November 2006)

Fessler, Pam. "Homeland Security Asset Report Inflames Critics." *All Things Considered* (12 July 2006). http://www.npr.org/templates/story/story.php?storyId=5552554 (accessed 7 November 2006).

Freeman, Linton C. "Centrality in Social Networks: Conceptual Clarification." *Social Networks*, 1 (1978/79): 215-239.
Friedkin, Noah E. "Horizons of Observability and Limits of Informal Social Control in Organizations." *Social Forces*, vol. 62, no. 1 (September 1983): 54-77.

Gerges, Fawaz A. *The Far Enemy: Why Jihad Went Global*. New York, NY: Cambridge University Press, 2005.

Gottfried, Ted. *Homeland Security vs. Constitutional Rights*. Brookfield, CT: Twenty-First Century Books, 2003.

Handel, Michael I. "Intelligence and the Problem of Strategic Surprise." In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*. Edited by Richard K. Betts and Thomas G. Mahnken, 1-58. Portland, OR: Frank Cass Publishers, 2003.

Hannan, Michael J., LCDR, USN. "Operational Net Assessment: A Framework for Social Network Analysis." *IOSPHERE* (Fall 2005): 27-32. http://www.au.af.mil/info-ops/iosphere/iosphere_fall05_hannan.pdf (accessed 6 June 2006).

Harary, Frank, Robert Z. Zorman and Dorwin Cartwright. *Structural Models: An Introduction to the Theory of Directed Graphs*. New York, NY: John Wiley & Sons, Inc., 1965.

Harmony Document AFGP-2002-000078. In Combating Terrorism Center. *Harmony and Disharmony: Exploiting al-Qa'ida's Organizational Vulnerabilities*. West Point, NY: Combating Terrorism Center, 14 February 2006.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence (Central Intelligence Agency): 1999. http://www.cia.gov/csi/books/19104/index.html (accessed 6 January 2006).

Heymann, Philip B. *Terrorism, Freedom, and Security: Winning without War*. Cambridge, Massachusetts: The MIT Press, 2003.

Hoffman, Bruce. "The Use of the Internet By [*sic*] Islamic Extremists." *CT-262-1: Testimony presented to the House Permanent Select Committee on Intelligence on May 4, 2006*. Santa Monica, CA: RAND, May 2006. http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf (accessed 12 November 2006).

Hubbard, Robert L. "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements." *Defense Intelligence Journal*, vol. 11, no. 1. (Winter 2002): 71-80.

IntelCenter. *Standing Assessment Brief on Most Likely Future Baseline Level Jihadi Attack Activity*. Alexandria, VA: IntelCenter, 7 August 2005. http://www.intelcenter.com/qaeda-charts.html (accessed 18 May 2006).

"Islamic Military Ideology [original title in Arabic]." *Al-Ommh*. http://www.alommh.net/forums/showthread.php?t=1629 (accessed 30 December 2005 and 5 January 2006). Cited in Center For International Issues Research. "Al-Qaida's Global Strategy Part 1 of 5: Antecedents and Evolution." *Global Issues Report* (30 August 2006) [electronic document].

Jackson, Brian A. "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda." *Studies in Conflict and Terrorism*, 29 (2006): 241-262.

Jacobsen, Annie. "Russian Airliners Were Likely Exploded from their Toilets." *WomensWallStreet.com*, 30 August 2004. http://www.womenswallstreet.com/WWS/article_landing.aspx?titleid=76&articleid=748 (accessed 6 November 2004).

Jenkins, Brian M. “International Terrorism.” In *Air Command and Staff College* text version 3.2, 9 vols. (Maxwell AFB, AL: Air University Press, 2000), vol. 2: *National and International Security Studies*, pp. 236-241. Previously published in *The Use of Force, Military Power and International Politics* (Rowan & Littlefield Publishers, Inc.).

Jenkins, Brian Michael. “Statement of Brian Michael Jenkins, Senior Advisor to the President of the RAND Corporation{,} Before the Senate Armed Services Subcommittee on Emerging Threats{,} November 15, 2001.” In *Terrorism: Current and Long Term Threats*, CT-187. Santa Monica, CA: RAND, 2001.

Jenkins, Brian Michael. *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*. Santa Monica, CA: RAND, 2002.

Jenkins, Brian Michael. *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*. Santa Monica, CA: RAND, 2006.

Jihadi recruitment video. Presented in “Understanding Islamist Militant Terrorism and Prevention Strategies.” First Technologies, LLC., Federal Law Enforcement Training Center, Glynco, GA. Training Seminar, 16-17 September 2004.

Jones, Morgan D. *The Thinker’s Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York, NY: Three Rivers Press, 1998.

Kauppi, Mark V. “Counterterrorism Analysis 101.” *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 39-53.

Khalsa, Sundri K., Captain, USAF. *Terrorism Forecasting: A Web-Based Methodology (Occasional Paper Number Eleven).* Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004.

Krebs, Valdis E. “Mapping Networks of Terrorist Cells.” *Connections* 24 (3): 43-52. http://www.insna.org/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf (accessed 17 May 2006).

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 3rd ed. Washington, DC: CQ Press, 2006.

MacDonald, Heather. “What We Don’t Know Can Hurt Us.” *City Journal*, 20 April 2004. http://www.city-journal.org/html/14_2_what_we_dont_know.html (accessed 17 Feb 2006) and http://www.frontpagemag.com/Articles/Printable.asp?ID=13053 (accessed 17 February 2006).

Mannes, Ariel Benjamin, Special Agent, Transportation Security Administration, Department of Homeland Security. "Interagency Intelligence Sharing and Analysis: Resources in the Homeland Security Reporting Process." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 20 October 2005.

Mao Tse-Tung. *Mao Tse-Tung on Guerilla Warfare*. Translated and with an introduction by Samuel B. Griffith. New York, NY: Praeger Publishers, Inc., 1961.

Mariani, Cliff. *Terrorism Prevention and Response: The Definitive Law Enforcement Guide to Prepare for Terrorist Activity*, 2nd Edition. New York, NY: Looseleaf Law Publications, Inc., 2004.

Marine Corps Institute. *ORM 1-0, Operational Risk Management.* Washington, DC: Headquarters Marine Corps, February 2002.

Martin, Gus. *Understanding Terrorism: Challenges, Perspectives, and Issues*. Thousand Oaks, CA: Sage Publications, Inc., 2003.

McCreary, John F., Defense Intelligence Agency. Presentation on Indications and Warning Analysis. Lecture with handouts. Naval Postgraduate School, Monterey, CA. Lecture, 22 February, 2006.

McCue, Colleen. "Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism." *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 48-60.

McDevitt, James J. "Summary of Indicator-Based-Methodology." Unpublished handout, n.p., n.d., provided in January 2002 at the Joint Military Intelligence College. Cited in Khalsa, Sundri K., Captain, USAF. *Terrorism Forecasting: A Web-Based Methodology (Occasional Paper Number Eleven).* Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004.

MetaMatrix: Tools for the Analysis of Organizational Structure. http://casos.isri.cmu.edu/projects/MetaMatrix/index.html (accessed 6 June 2006).

Miles, Raymond E., and Charles C. Snow. *Organizational Strategy, Structure, and Process*. New York, NY: McGraw-Hill, Inc., 1979.

Military Studies in the Jihad against the Tyrants [a.k.a. *The al-Qa'eda Terrorist Training Manual* or *The Encyclopedia of Jihad*.] [Attributed to Al-Qa'eda, ca. 1992 or 1993, translated by the Manchester Constabulary, UK, ca. 2002]. http://www.thesmokinggun.com/archive/jihadmanual.html (accessed 10 March 2006).

Miller, Gary J. *Managerial Dilemmas: The Political Economy of Hierarchy*. New York, NY: Cambridge University Press, 1992.

MSNBC. “Inspector: Homeland Security Database Flawed.” *MSNBC News Services* (12 July 2006). http://www.msnbc.msn.com/id/13822662/ (accessed 7 November 2006).

Naji, Abu Bakr. *The Management of Savagery*. Translated by William McCants. [West Point, NY: Combating Terrorism Center] and [Cambridge, MA]: John M. Olin Institute for Strategic Studies, 23 May 2006.

Nasr, Seyyed Vali Reza. Series of lectures on Islamic Fundamentalism at the Naval Postgraduate School, Monterey, CA, 25 September-23 October 2006.

“The Nation is Coming [original title in Arabic].” *Al-Ommh*. http://www.alommh.net/forums/showthread.php?t=1694 (accessed 30 December 2005 and 5 January 2006). Cited in Center For International Issues Research. “Al-Qaida’s Global Strategy Part 1 of 5: Antecedents and Evolution.” *Global Issues Report* (30 August 2006) [electronic document].

Odisho, Joseph, U.S. Government contract linguist. Personal conversation during USAF Special Investigations Academy Critical Threat Counterintelligence Collections Course, 2005.

Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terrorism*. New York, NY: Random House, 2005.

Peters, Ralph. “The Case for Human Intelligence.” *Armed Forces Journal* (July 2005): 24-26.

Philpott, Don. “The London Bombings: New Evidence Points to Al-Qaida and a New Terror Campaign.” *Homeland Defense Journal Special Report*, [2005]. http://www.homelanddefensejournal.com/pdfs/LondonBombing_SpecialReport.pdf (accessed 5 November 2006).

Pillar, Paul R. “Fighting International Terrorism: Beyond September 11th.” *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 17-26.

Pillar, Paul. *Terrorism and U.S. Foreign Policy*, paperback edition. Washington, DC: Brookings Institution Press, 2003.

Posner, Gerald. *Why America Slept: The Failure to Prevent 9/11*. New York, NY: Random House, 2003.

Ranstorp, Magnus. “Statement of Magnus Ranstorp to the National Commission on Terrorist Attacks Upon the United States March 31, 2003.” http://www.allamericanpatriots.com/m-wfsection+print+articleid-760.html (accessed 4 November 2006).

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). "Terrorism & Attacks on the Civil Aviation Industry." International Counter-Terrorism Officers [*sic*] Association 2nd Annual Conference, Las Vegas, NV. Lecture, 29 September 2004.

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). "Understanding Terrorist Ideology." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). "Issues in Transportation Related [*sic*] Terrorism." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 20 October 2005.

Roth, John, Douglas Greenburg and Serena Wille. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*. Washington, DC: U.S. Government Printing Office, 2004 [electronic document].

Rowland, John C. "The New Terrorism: Global Jihad." International Counter-Terrorism Officers [*sic*] Association 2nd Annual Conference, Las Vegas, NV. Lecture, 28 September 2004.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press, 2004.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York, NY: Copernicus Books, 2003.

Seifert, Jeffrey W. "Data Mining: An Overview." *The Library of Congress CRS Report RL31798*. Washington, DC: Congressional Research Service (CRS Web), 7 June 2005.

Shahar, Yael. "London Underground Partially Shut Down after Minor Explosions." The Institute for Counter-Terrorism, 21 July 2005. http://www.ict.org.il/spotlight/det.cfm?id=1094 (accessed 5 November 2006).

Shapiro, Jacob N. *Organizing Terror: Hierarchy and Networks in Covert Operations*. Working paper, Stanford University, 1 November 2005.

Shulsky, Abram N. and Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. Washington, DC: Brassey's, Inc., 2002.

Sloan, Stephen. *Beating International Terrorism: An Action Strategy for Preemption and Punishment*, revised edition. Maxwell AFB, AL: Air University Press, 2002.

Sparrow, Malcolm K. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks*, 13 (1991): 251-274.

Spyer, Jonathan. “The Al-Qa’ida Network and Weapons of Mass Destruction.” *Middle East Review of International Affairs*, vol. 8, no. 4 (September 2004): 29-45. http://meria.idc.ac.il/journal/2004/issue3/spyer.pdf (accessed 4 November 2006).

“Strategy of Al-Qaida [original title in Arabic].” *Al-Ommh*. http://www.alommh.net/estra.htm (accessed 29 December 2005 and 5 January 2006). Cited in Center For International Issues Research. “Al-Qaida’s Global Strategy Part 1 of 5: Antecedents and Evolution.” *Global Issues Report* (30 August 2006) [electronic document].

Suspected terrorist pre-operational reconnaissance video, seized by Canadian authorities. Presented by Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). “Understanding Terrorist Ideology.” International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Teft, Bruce. “Terrorism Awareness—Islamic Terrorism: Origins and Prevention.” International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Thomas, Troy S., Major, USAF. *Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism.* Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004.

U.S. Department of Homeland Security Office of the Inspector General. “Progress in Developing the National Asset Database.” [OIG Report] *OIG-06-40*. Washington, DC: U.S. Government Printing Office, June 2006.

U.S. Government Counterterrorist Training Group Special Seminar on Surveillance Detection, September-October 1997.

“Vulnerabilities in the Terrorist Attack Cycle.” *STRATFOR* (Strategic Forecasting, Inc.), 29 September 2005. http://www.stratfor.com/products/premium/print.php?storyId=256319 (accessed 6 March 2006).

Webster’s Ninth New Collegiate Dictionary. Springfield, MA: Merriam-Webster, Inc., 1987.

White, Jonathan R. *Defending the Homeland: Domestic Intelligence, Law Enforcement and Security.* Canada: Wadsworth/Thomson, 2004.

Wijninga, Peter W.W., Lt Col, Royal Netherlands Air Force, and Richard Szafranski. “Beyond Utility Targeting: Toward Axiological Air Operations.” *Aerospace Power Journal* (Winter 2000): 45-59.

Zanini, Michele, and Sean J.A. Edwards. “The Networking of Terror in the Information Age.” In *Networks and Netwar: The Future of Terror, Crime and Militancy*, edited by John Arquilla John and David Ronfeldt, 29-60. Santa Monica, CA: RAND, 2001.

Zawahiri, Ayman al-. Letter to Abu Musab al-Zarqawi [translated], 9 Jul 2005. http://www.weeklystandard.com/Content/Public/Articles/000/000/006/203gpuul.asp (accessed 31 May 2006).

Zawahiri, Ayman al-. Electronic mail to Muhammad Atef [translated], 15 April 1999. In Cullison, Alan. “Inside Al-Qaeda’s Hard Drive.” *The Atlantic Monthly* (September 2004). http://www.theatlantic.com/doc/200409/cullison (accessed 3 November 2006).

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Published Books

Anonymous. *A Law Enforcement Guide to Understanding Islamist Terrorism*. Baton Rouge, LA: First Capital Technologies, LLC., 2003.

Armstrong, Karen. *The Battle For God: A History of Fundamentalism*. New York, NY: Ballantine Books (Random House), 2001.

Bell, J. Bowyer. *The IRA 1968-2000: Analysis of a Secret Army*. New York, NY: Frank Cass Publishers, 2000.

Bergen, Peter L. *Holy War, Inc.: Inside the Secret World of Osama bin Laden*. New York, NY: The Free Press (Simon & Schuster, Inc.), 2001.

Bergen, Peter L. *Holy War, Inc.: Inside the Secret World of Osama bin Laden*, First Touchstone Edition. New York, NY: Touchstone (Simon & Schuster, Inc.), 2002.

Bermudez, Joseph S., Jr. *Terrorism: the North Korean Connection*. New York, NY: Crane Russack (Taylor & Francis New York, Inc.), 1990.

Bolz, Frank Jr.; Dudonis, Kenneth J.; and Schulz, David P. *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. Boca Raton, FL: CRC Press LLC, 2002.

Brisard, Jean-Charles. *Zarqawi: The New Face of Al-Qaeda*. In collaboration with Damien Martinez. (Translated from French.) New York, NY: Other Press, 2005. Originally published as *Zarkaoui, le nouveau visage d'Al-Qaida* ([France]: Librairie Arthème Fayard, 2005).

Burke, Jason. *Al-Qaeda: Casting a Shadow of Terror*. London, UK: I.B. Tauris & Co. Ltd., 2003.

Burke, Jason. *Al-Qaeda: The True Story of Radical Islam*. New York, NY: I.B. Tauris & Co. Ltd., 2004.

Davis, Paul K. and Brian Michael Jenkins. *Deterrence & Influence in Counterterrorism: A Component in the War on al Qaeda*. Santa Monica, CA: RAND National Defense Research Institute, 2002.

Defeating the Jihadists: A Blueprint for Action. Century Foundation Task Force. Richard A. Clarke, chairman. New York, NY: The Century Foundation Press, 2004.

Ehrenfeld, Rachel. *Funding Evil: How Terrorism Is Financed—and How to Stop It*. Chicago, IL (printed in Canada): Bonus Books, 2003.

Frum, David and Richard Perle. *An End to Evil: How to Win the War on Terror*. New York, NY: Random House, Inc., 2003.

Gerges, Fawaz A. *The Far Enemy: Why Jihad Went Global*. New York, NY: Cambridge University Press, 2005.

Gottfried, Ted. *Homeland Security vs. Constitutional Rights*. Brookfield, CT: Twenty-First Century Books, 2003.

Harary, Frank, Robert Z. Zorman and Dorwin Cartwright. *Structural Models: An Introduction to the Theory of Directed Graphs*. New York, NY: John Wiley & Sons, Inc., 1965.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence (Central Intelligence Agency): 1999. http://www.cia.gov/csi/books/19104/index.html (accessed 6 January 2006).

Heymann, Philip B. *Terrorism, Freedom, and Security: Winning without War*. Cambridge, Massachusetts: The MIT Press, 2003.

Hoffman, Bruce. *Inside Terrorism*. New York, NY: Columbia University Press, 1998.

Jenkins, Brian Michael. *Countering al Qaeda: An Appreciation of the Situation and Suggestions for Strategy*. Santa Monica, CA: RAND, 2002.

Jenkins, Brian Michael. *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*. Santa Monica, CA: RAND, 2006.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*. New York, NY: Three Rivers Press, 1998.

Kepel, Gilles. *Jihad: The Trail of Political Islam*. Translated by Anthony F. Roberts. Cambridge, MA: The Belknap Press of Harvard University Press, 2002.

Kessler, Ronald. *The CIA at War: Inside the Secret Campaign Against Terror*. New York, NY: St. Martin's Press, 2003.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 3rd ed. Washington, DC: CQ Press, 2006.

Mao Tse-Tung. *Mao Tse-Tung on Guerilla Warfare*. Translated and with an introduction by Samuel B. Griffith. New York, NY: Praeger Publishers, Inc., 1961.

Mariani, Cliff. *Terrorism Prevention and Response: The Definitive Law Enforcement Guide to Prepare for Terrorist Activity*, 2nd Edition. New York, NY: Looseleaf Law Publications, Inc., 2004.

Marine Corps Institute. *ORM 1-0, Operational Risk Management*. Washington, DC: Headquarters Marine Corps, February 2002.

Martin, Gus. *Understanding Terrorism: Challenges, Perspectives, and Issues*. Thousand Oaks, CA: Sage Publications, Inc., 2003.

Miles, Raymond E., and Charles C. Snow. *Organizational Strategy, Structure, and Process*. New York, NY: McGraw-Hill, Inc., 1979.

Military Studies in the Jihad against the Tyrants [a.k.a. *The al-Qa'eda Terrorist Training Manual* or *The Encyclopedia of Jihad*.] [Attributed to Al-Qa'eda, ca. 1992 or 1993, translated by the Manchester Constabulary, UK, ca. 2002]. http://www.thesmokinggun.com/archive/jihadmanual.html (accessed 10 March 2006).

Miller, Gary J. *Managerial Dilemmas: The Political Economy of Hierarchy*. New York, NY: Cambridge University Press, 1992.

Naji, Abu Bakr. *The Management of Savagery*. Translated by William McCants. [West Point, NY: Combating Terrorism Center] and [Cambridge, MA]: John M. Olin Institute for Strategic Studies, 23 May 2006.

Napoleoni, Loretta. *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. Sterling, VA: Pluto Press, 2003.

Pape, Robert A. *Dying to Win: The Strategic Logic of Suicide Terrorism*. New York, NY: Random House, 2005.

Pillar, Paul. *Terrorism and U.S. Foreign Policy*, paperback edition. Washington, DC: Brookings Institution Press, 2003.

Posner, Gerald. *Why America Slept: The Failure to Prevent 9/11*. New York, NY: Random House, 2003.

Rand McNally Road Atlas Deluxe Edition (Skokie, IL: Rand McNally & Company, 1998).

Sageman, Marc. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press, 2004.

Schauer, Frederick. *Profiles, Probabilities and Stereotypes*. Cambridge, MA: The Belknap Press of Harvard University Press, 2003.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York, NY: Copernicus Books, 2003.

Shulsky, Abram N. and Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence*, 3rd ed. Washington, DC: Brassey's, Inc., 2002.

Sloan, Stephen. *Beating International Terrorism: An Action Strategy for Preemption and Punishment*, revised edition. Maxwell AFB, AL: Air University Press, 2002.

Thomas, Troy S., Major, USAF. *Beneath the Surface: Intelligence Preparation of the Battlespace for Counterterrorism.* Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004.

Thome, L. *Anti-Terrorism 101: A Primer for Protection*. McKinney, TX: TDM Publishing, 2001.

Webster's Ninth New Collegiate Dictionary. Springfield, MA: Merriam-Webster, Inc., 1987.

Weldon, Curt, Congressman, U.S. House of Representatives. *Countdown to Terror*. Washington, DC: Regnery Publishing, Inc., 2005.

White, Jonathan R. *Defending the Homeland: Domestic Intelligence, Law Enforcement and Security.* Canada: Wadsworth/Thomson, 2004.

Articles and Chapters Published in Collected Works and Anthologies

Arquilla, John, and David Ronfeldt. "The Advent of Netwar (Revisited)." In *Networks and Netwar: The Future of Terror, Crime and Militancy*, edited by John Arquilla John and David Ronfeldt, 1-27. Santa Monica, CA: RAND, 2001.

Cole, David and Dempsey, James X. "Ethnic Profiling Is Unfair and Ineffective." In *Homeland Security*, edited by James D. Torr. San, Diego, CA: Greenhaven Press, 2004.

Conway, Maura. "Terrorism and IT: Cyberterrorism and Terrorist Organizations Online." In *Terrorism and Counterterrorism: Understanding the New Security Environment*, eds. Russell D. Howard and Reid L. Sawyer. Guilford, CT: McGraw-Hill/Dushkin, 2004.

Handel, Michael I. "Intelligence and the Problem of Strategic Surprise." In *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel.* Edited by Richard K. Betts and Thomas G. Mahnken, 1-58. Portland, OR: Frank Cass Publishers, 2003.

Jenkins, Brian M. "International Terrorism." In *Air Command and Staff College* text version 3.2, 9 vols. (Maxwell AFB, AL: Air University Press, 2000), vol. 2: *National and*

International Security Studies, pp. 236-241. Previously published in *The Use of Force, Military Power and International Politics* (Rowan & Littlefield Publishers, Inc.).

Kayyem, Juliette. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning." In Howitt, Arnold M. and Pangi, Robyn L., Ed. *Countering Terrorism: Dimensions of Preparedness*. Cambridge, MA: The MIT Press, 2003.

Kinsley, Michael. "Ethnic Profiling to Prevent Terrorism Is Justified." In *Homeland Security*, edited by James D. Torr. San, Diego, CA: Greenhaven Press, 2004.

McCaffrey, Barry R., General, USA (Retired) and Basso, John A., Major, USA. "Narcotics, Terrorism, and International Crime: The Convergence Phenomenon." In *Terrorism and Counterterrorism: Understanding the New Security Environment*, edited by Russell D. Howard, Colonel, USA and Reid L. Sawyer, Major, USA. Guilford, CT: McGraw-Hill/Dushkin, 2004. [McCaffrey and Basso's article originally published in 2003.]

Zanini, Michele, and Sean J.A. Edwards. "The Networking of Terror in the Information Age." In *Networks and Netwar: The Future of Terror, Crime and Militancy*, edited by John Arquilla John and David Ronfeldt, 29-60. Santa Monica, CA: RAND, 2001.

U.S. Government Commissions

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. Bridgewater, NJ: Replica Books (Baker & Taylor), 2004. (Originally published: Washington, DC: U.S. Government Printing Office, 2004).

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, authorized Edition [paperback]. New York, NY: W.W. Norton & Company, Inc., [2004].

The 9/11Commission Report, National Commission on Terrorist Attacks Upon the United States. Thomas H. Kean, chairman. Washington, DC: U.S. Government Printing Office, 2004. (Electronic document.)

Eldridge, Thomas R.; Ginsburg, Susan; Hempel, Walter T. II; Kephart, Janice L.; and Moore, Kelly. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, DC: 2004. (Electronic version.)

Independent Review of the Khobar Towers Bombing, Unclassified Parts A and B. Headquarters 12th Air Force, by James F. Record. Maxwell AFB, AL: Air University, 31 October 1996. http://www.au.af.mil/au/awc/awcgate/khobar/recordf.htm (accessed 17 February 2006).

"Recommendation from Initial Report dated September 9, 1996." *White House Commission on Aviation Safety and Security: Final Report to President Clinton.* Vice President Al Gore, chairman. Washington, DC: 1997. http://www.fas.org/irp/threat/212fin~1.html (accessed 17 February 2006).

Report of the DOD Commission on Beirut International Airport Terrorist Act, October 23, 1983. Washington, DC: US Government Printing Office, 20 December 1983. http://www.ibiblio.org/hyperwar/AMH/XX/MidEast/Lebanon-1982-1984/DOD-Report/ (accessed 17 February 2006).

Roth, John, Douglas Greenburg and Serena Wille. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*. Washington, DC: U.S. Government Printing Office, 2004 [electronic document].

Published Testimony

Jenkins, Brian Michael. "Statement of Brian Michael Jenkins, Senior Advisor to the President of the RAND Corporation{,} Before the Senate Armed Services Subcommittee on Emerging Threats{,} November 15, 2001." In *Terrorism: Current and Long Term Threats*, CT-187. Santa Monica, CA: RAND, 2001.

Hoffman, Bruce. "The Use of the Internet By [*sic*] Islamic Extremists." *CT-262-1: Testimony presented to the House Permanent Select Committee on Intelligence on May 4, 2006*. Santa Monica, CA: RAND, May 2006. http://www.rand.org/pubs/testimonies/2006/RAND_CT262-1.pdf (accessed 12 November 2006).

Sageman, Marc. "Statement of Marc Sageman to the National Commission on Terrorist Attacks Upon the United States, July 9, 2003." http://www.globalsecurity.org/security/library/congress/9-11_commission/030709-sageman.htm (accessed 17 February 2006).

Ranstorp, Magnus. "Statement of Magnus Ranstorp to the National Commission on Terrorist Attacks Upon the United States March 31, 2003." http://www.allamericanpatriots.com/m-wfsection+print+articleid-760.html (accessed 4 November 2006).

"Substitution for the Testimony of Khalid Sheikh Mohammed, Defendant's Exhibit 941." *U.S. v. Moussaoui*. Cr. No. 01-455-A [28 March 2006]. http://www.rcfp.org/moussaoui/pdf/DX-0941.pdf (accessed 31 May 2006).

Analysis and Academic Research Reports (Government and Private)

"Al-Qaeda: The Many Faces of an Islamist Extremist Threat." *Report of the House Permanent Select Committee on Intelligence* (Washington, DC: U.S. Government Printing Office, June 2006).

Armanios, Febe. "The Islamic Traditions of Wahhabism and Salafiyya." *The Library of Congress CRS Report RS21695*. Washington, DC: Congressional Research Service (CRS Web), 22 December 2003.

Beech, Michael F., LTC, U.S. Army. "Observing al Qaeda through the Lens of Complexity Theory: Recommendations for the National Strategy to Defeat Terrorism." [*U.S. Army War College Center for Strategic Leadership*] *Student Issue Paper*, vol. 204-01 (July 2004).

Best, Richard A. "Intelligence to Counter Terrorism: Issues for Congress." *The Library of Congress CRS Report RL31292*. Washington, DC: Congressional Research Service (CRS Web), 27 May 2003.

Blanchard, Christopher M. "Al Qaeda: Statements and Evolving Ideology." *The Library of Congress CRS Report RS21973*. Washington, DC: Congressional Research Service (CRS Web), 16 November 2004.

Blanchard, Christopher M. "Islamic Religious Schools, *Madrasas*: Background." *The Library of Congress CRS Report RS21654*. Washington, DC: Congressional Research Service (CRS Web), 10 January 2006.

Borgatti, Stephen P., Kathleen M. Carley and David Krackhardt. *On the Robustness of Centrality Measures under Conditions of Imperfect Data*. Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d. http://www.analytictech.com/borgatti/papers/robustness.pdf (accessed 6 Jun 2006).

Brachman, Jarret M. and William F. McCants. *Stealing Al-Qaida's Playbook*. West Point, NY: Combating Terrorism Center, February 2006.

Carley, Kathleen M. *Estimating Vulnerabilities in Large Covert Networks*. Dynamic Networks project paper, Carnegie Mellon University, Pittsburgh, PA, n.d. http://www.dodccrp.org/events/2004/CCRTS_San_Diego/CD/papers/249.pdf (accessed 6 June 2006).

[Case Study on the 1998 Bombings of the U.S. Embassies in Kenya and Tanzania (from Federal Investigation and Federal Trial Transcripts).] *Defense Intelligence Assessment DITSUM-103-01*. Washington, DC: Defense Intelligence Agency, 30 May 2001.

Center for International Issues Research. “Al-Qaida’s Global Strategy Part 1 of 5: Antecedents and Evolution.” *Global Issues Report* (30 August 2006) [electronic document].

Center for International Issues Research. “Al-Qaida’s Global Strategy Part 2 of 5: Phase 1 ‘The Awakening.’” *Global Issues Report* (2 October 2006) [electronic document].

Center for International Issues Research. “Al-Qaida’s Global Strategy Part 3 of 5: Phase 2 ‘Opening the Eyes’ Implementation.” *Global Issues Report* (6 October 2006) [electronic document].

Center for International Issues Research. “Al-Qaida’s Global Strategy Part 4 of 5: Planning for the Future—Phases Four to Seven.” *Global Issues Report* (6 October 2006) [electronic document].

Center for International Issues Research. “Al-Qaida’s Global Strategy Part 5 of 5: Comparison of Al-Qaida’s Seven-Phase Strategy with ‘The Management of Savagery.’” *Global Issues Report* (30 August 2006) [electronic document].

Center for International Issues Research. “Militant Sunni Websites Denounce Hezbollah as Israeli / USG ‘Agent.’” *Global Issues Report* (19 July 2006) [electronic document].

Center for International Issues Research. “Postings Cite U.S. ‘Economic Weakness,’ Call for ‘Economic Jihad.’” *Global Issues Report* (27 September 2006) [electronic document].

Combating Terrorism Center. *Harmony and Disharmony: Exploiting al-Qa’ida’s Organizational Vulnerabilities*. West Point, NY: Combating Terrorism Center, 14 February 2006.

Harmony Document AFGP-2002-000078. In Combating Terrorism Center. *Harmony and Disharmony: Exploiting al-Qa’ida’s Organizational Vulnerabilities*. West Point, NY: Combating Terrorism Center, 14 February 2006.

IntelCenter. *Standing Assessment Brief on Most Likely Future Baseline Level Jihadi Attack Activity.* Alexandria, VA: IntelCenter, 7 August 2005. http://www.intelcenter.com/qaeda-charts.html (accessed 18 May 2006).

Khalsa, Sundri K., Captain, USAF. *Terrorism Forecasting: A Web-Based Methodology (Occasional Paper Number Eleven).* Washington, DC: Center for Strategic Intelligence Research, Joint Military Intelligence College, November 2004.

Leiken, Robert S. *Bearers of Global Jihad? Immigration and National Security after 9/11*. Washington, DC: The Nixon Center, 2004.

Marrin, Stephen. “Homeland Security and the Analysis of Foreign Intelligence.” Markle Foundation Task Force on National Security in the Information Age, 15 July 2002.

McCreary, John F., Defense Intelligence Agency. *Intelligence as Evidence: A J2 Analyst Aid*. Bolling AFB, DC: Defense Intelligence Agency, July 2003.

MetaMatrix: Tools for the Analysis of Organizational Structure. http://casos.isri.cmu.edu/projects/MetaMatrix/index.html (accessed 6 June 2006).

Moniquet, Claude. "One Year After The London Bomb Attacks, More Questions Than Answers." *Background Analysis 07/07/2006*. European Strategic Intelligence and Security Center: 07 July 2006, http://www.esisc.net/London%20note.pdf (accessed 31 October 2006).

Post, Patrick M., and Harjit Singh Sandhu. *The Hawala Alternative Remittance System and its Role in Money Laundering*. Financial Crimes Enforcement Network and INTERPOL/FOPAC, 2000.

Seifert, Jeffrey W. "Data Mining: An Overview." *The Library of Congress CRS Report RL31798*. Washington, DC: Congressional Research Service (CRS Web), 7 June 2005.

Shapiro, Jacob N. *Organizing Terror: Hierarchy and Networks in Covert Operations*. Working paper, Stanford University, 1 November 2005.

Steinberg, James B.; Graham, Mary; and Eggers, Andrew. "Building Intelligence to Fight Terrorism." *Policy Brief* No. 125. Washington, DC: The Brookings Institution, September 2003.

U.S. Department of Homeland Security Office of the Inspector General. "Progress in Developing the National Asset Database." [OIG Report] *OIG-06-40*. Washington, DC: U.S. Government Printing Office, June 2006.

U.S. Department of State. *Patterns of Global Terrorism 1999*. Washington, DC: U.S. Government Printing Office, 1999.

U.S. Department of State Office of the Coordinator for Counterterrorism. *Country Reports on Terrorism 2005*. Washington, DC: U.S. Government Printing Office, April 2006.

Professional Journals

Anonymous. "Where is Defense HUMINT in America's New War?" *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 81-89.

Arquilla, John, and David Ronfeldt. "The Underside of Netwar." *Review – Institute of Public Affairs* (December 2002): 3-5.

Autera, Joseph. “Before It Makes the Headlines: Effective Threat Detection Strategies and Tactics.” *Journal of Counterterrorism and Homeland Security Studies* (Fall 2003): 36-43.

Bodrero, D. Douglas. “Law Enforcement’s Challenge to Investigate, Interdict, and Prevent Terrorism.” *The Police Chief* (February 2002): 41-48.

Cainkar, Louise. “Post 9/11 Domestic Policies Affecting U.S. Arabs and Muslims: A Brief Review.” *Comparative Studies of South Asia, Africa and the Middle East*, 24:1 (2004): 245-248. http://muse.jhu.edu/demo/comparative_studies_of_south_asia_africa_and_the_middle_east/v024/24.1cainkar02.pdf (accessed 17 February 2006).

Carroll, Thomas Patrick. “The CIA and the War on Terror.” *Middle East Intelligence Bulletin*, vol. 4 no. 9 (September 2002). http://www.meib.org/articles/0209_me2.htm (accessed 17 February 2006).

Crenshaw, Martha. “The Causes of Terrorism.” *Comparative Politics* (July 1981): 379-399.

Dowling, Thomas. “Failures of Imagination: Thoughts on the 9/11 Commission Report.” *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 7-16.

Freeman, Linton C. “Centrality in Social Networks: Conceptual Clarification.” *Social Networks*, 1 (1978/79): 215-239.

Friedkin, Noah E. “Horizons of Observability and Limits of Informal Social Control in Organizations.” *Social Forces*, vol. 62, no. 1 (September 1983): 54-77.

Hannan, Michael J., LCDR, USN. “Operational Net Assessment: A Framework for Social Network Analysis.” *IOSPHERE* (Fall 2005): 27-32. http://www.au.af.mil/info-ops/iosphere/iosphere_fall05_hannan.pdf (accessed 6 June 2006).

Horgan, John, and Max Taylor. “Playing the ‘Green Card’—Financing the Provisional IRA: Part 2.” *Terrorism and Violence*, vol. 15, no. 2 (Summer 2003).

Hubbard, Robert L. “Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements.” *Defense Intelligence Journal*, vol. 11, no. 1. (Winter 2002): 71-80.

Innes, Martin. “Policing Uncertainty: Countering Terror through Community Intelligence and Democratic Policing.” *The Annals of the American Academy*, no. 605 (May 2006): 222-241.

Jackson, Brian A. “Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda.” *Studies in Conflict and Terrorism*, 29 (2006): 241-262.

Kauppi, Mark V. “Counterterrorism Analysis 101.” *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 39-53.

Krebs, Valdis E. “Mapping Networks of Terrorist Cells.” *Connections* 24 (3): 43-52. http://www.insna.org/Connections-Web/Volume24-3/Valdis.Krebs.web.pdf (accessed 17 May 2006).

Leiken, Robert S. “Europe’s Angry Muslims.” *Foreign Affairs* [online version] (July/August 2005). http://www.foreignaffairs.org/20050701faessay84409-p50/robert-s-leikin/europe-s-angry-muslims.html (accessed 17 February 2006)

McCue, Colleen. “Data Mining and Predictive Analytics: Battlespace Awareness for the War on Terrorism.” *Defense Intelligence Journal*, vol. 13, no. 1 & 2 (2005): 48-60.

Olson, James. “The 10 Commandments of Counterintelligence.” *Studies of Intelligence* (Unclassified Edition), Fall-Winter 2001, No.11, Central Intelligence Agency Center for the Study of Intelligence. http://www.cia.gov/csi/studies/fall_winter_2001/article08.html (accessed 17 February 2006) and http://www.cicentre.com/Documents/DOC_CI_10_Commandments.htm (accessed 17 February 2006).

Peters, Ralph. “The Case for Human Intelligence.” *Armed Forces Journal* (July 2005): 24-26.

Pillar, Paul R. “Fighting International Terrorism: Beyond September 11th.” *Defense Intelligence Journal*, vol. 11, no. 1 (Winter 2002): 17-26.

Rashid, Ahmed. “The Taliban: Exporting Extremism.” *Foreign Affairs*, vol. 78, no. 6 (November/December 1999): 22-35.

Schramm, Matthias, and Markus Taube. “Evolution and Institutional Foundation of the *Hawala* Financial System.” *International Review of Financial Analysis* 12 (2003): 405-420.

Sparrow, Malcolm K. “The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects.” *Social Networks*, 13 (1991): 251-274.

Spooner, Major General Richard E. “The Patriot Act.” *Defense Intelligence Journal*, vol. 12, no. 2 (2003): 97-102.

Spyer, Jonathan. “The Al-Qa’ida Network and Weapons of Mass Destruction.” *Middle East Review of International Affairs*, vol. 8, no. 4 (September 2004): 29-45. http://meria.idc.ac.il/journal/2004/issue3/spyer.pdf (accessed 4 November 2006).

Wijninga, Peter W.W., Lt Col, Royal Netherlands Air Force, and Richard Szafranski. “Beyond Utility Targeting: Toward Axiological Air Operations.” *Aerospace Power Journal* (Winter 2000): 45-59.

News Media, Internet Magazines and Other Internet Sources

“A Blow Against Racial Profiling,” Center for Constitutional Rights. http://www.ccr-ny.org/v2/reports/report.asp?ObjID=Jk5uXqHbDE&Content=161 (accessed 27 March 2006).

ABC News. “Militant Britain: Radical Muslims Born or Based in Britain Are Making Militant Waves.” 29 Dec 2003. http://www.ds-osac.org/view.cfm?key=7E4552434B56&type=2B170C1E0A3A0F162820 (accessed 1 February 2004).

Anderson, John Ward and Karen DeYoung. “Plot to Bomb U.S.-Bound Jets Is Foiled: Britain Arrests 24 Suspected Conspirators.” *Washington Post Foreign Service* (11 August 2006). http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html?referrer=email (accessed 3 October 2006).

Arquilla, John, and David Ronfeldt. “Networks, Netwars, and the Fight for the Future.” *First Monday*, vol. 6, no. 10 (September 2001). http://www.firstmonday.org/issues/issue6_10/ronfeldt/ (accessed 19 May 2006).

Auster, Lawrence. “How to Fight Jihad in America.” *FrontPageMagazine.com*, 26 May 2004. http://www.frontpagemag.com/Articles/ReadArticles.asp?ID=13532 (accessed 24 November 2005).

Boyle, Jon and Trevelyan, Mark. “Al Qaeda exploits 'blue-eyed' Muslim converts [*sic*].” Reuters on CNN.com (Cable News Network), 20 September, 2005. http://cnn.netscape.cnn.com/news/story.jsp?idq=/ff/story/0002%2F20051014%2F0841831103.htm&photoid=20050920LON005D&ewp=ewp_news_qaeda (accessed 14 October 2005).

Burton, Fred. “Al Qaeda in 2006: Devolution and Adaptation.” *STRATFOR* (Strategic Forecasting, Inc.), 3 January 2006. http://www.stratfor.com/products/premium/print.php?storyId=260353 (accessed 18 February 2006).

Burton, Fred. “Al Qaeda: Targeting Guidance and Timing.” *Stratfor*, 9 December 2005. http://www.stratfor.com/products/premium/read_article.php?id=259453 (accessed 18 February 2006).

Burton, Fred. “Beware of ‘Kramer’: Tradecraft and the New Jihadists.” *STRATFOR* (Strategic Forecasting, Inc.), 18 January 2006. http://www.stratfor.com/products/premium/read_article.php?id=261022 (accessed 16 February 2006).

Burton, Fred. “The Problem of HUMINT.” *STRATFOR* (Strategic Forecasting, Inc.), 4 August 2005. http://www.stratfor.biz/Print.neo?storyId=253073 (accessed 18 February 2006).

Burton, Fred. “The Psychological Battlefield.” *STRATFOR* (Strategic Forecasting, Inc.), 10 August 2005. http://www.stratfor.com/products/premium/read_article.php?id=253467 (accessed 18 February 2006).

Calabresi, Massimo and Ratnesar, Romesh. “Can We Stop the Next Attack?” *Time*, 11 April 2002 [via Nexis-Lexis].

Coll, Steve and Glasser, Susan B. “e-QAEDA: From Afghanistan to the Internet—Terrorists Turn to Web as Base of Operations.” *The Washington Post*, Sunday, 7 August 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (accessed 4 November 2006).

Cullison, Alan. “Inside Al-Qaeda’s Hard Drive.” *The Atlantic Monthly* (September 2004). http://www.theatlantic.com/doc/200409/cullison (accessed 3 November 2006).

“Dire Prediction From Osama's Bodyguard.” *60 Minutes*. (CBS Corporation [Columbia Broadcast System]: 2 April 2006). http://www.cbsnews.com/stories/2006/03/30/60minutes/printable1457859.shtml (accessed 2 April 2006).

Farah, Douglas, and Peter Finn. “Terrorism Inc.; Al Qaeda Franchises Brand of Violence to Groups Across World.” *Washington Post*, 21 November 2003. http://www.washingtonpost.com/ac2/wp-dyn/A1934-2003Nov20?language=printer (accessed 9 December 2006).

“FBI leads bombing investigation; security warnings reviewed.” *CNN.com*, 13 August 1998. http://www.cnn.com/WORLD/africa/9808/13/embassy.fbi.03/ (accessed 21 May 2006).

Federal Bureau of Investigation. “Most Wanted Terrorists.” [Official government web site.] http://www.fbi.gov/wanted/terrorists/teraladel.htm (accessed 3 November 2006)

Fessler, Pam. “Homeland Security Asset Report Inflames Critics.” *All Things Considered* (12 July 2006). http://www.npr.org/templates/story/story.php?storyId=5552554 (accessed 7 November 2006).

Fox News. “Islamic Recruiters Target Potential Jihadees,” 26 November 2004. Steve Harrigan, correspondent. http://www.foxnews.com/story/0,2933,139709,00.html (accessed 17 February 2006).

Gerecht, Reuel Marc. “The Counterrorist Myth.” *The Atlantic Monthly*, July/August 2001. http://www.theatlantic.com/doc/prem/200107/gerecht (accessed 17 February 2006).

Horne, Jennifer. “Legislative Alert: Congress Considers New Measures to Ban Alleged Profiling.” *Legislative Activities* (web site). International Association of Chiefs of Police, [2001]. http://www.theiacp.org/documents/index.cfm?document_id=44&fuseaction=document&subtype_id= (accessed 12 November 2006).

Jacobsen, Annie. “Russian Airliners Were Likely Exploded from their Toilets.” *WomensWallStreet.com*, 30 August 2004. http://www.womenswallstreet.com/WWS/article_landing.aspx?titleid=76&articleid=748 (accessed 6 November 2004).

Jacobsen, Annie. “Terror in the Skies—Again?” *WomensWallStreet.com*, 13 July 2004. http://www.womenswallstreet.com/WWS/article_landing.aspx?titleid=76&articleid=711 (accessed 6 November 2004).

Johnson, James Turner. “Jihad and Just War.” *First Things*, No. 124. June/July 2002. http://www.firstthings.com/ftissues/ft0206/opinion/johnson.html (accessed 17 February 2006).

Kalugin, Oleg D. “Terrorism and Human Intelligence.” Center for Counterterrorism Studies/Center for Counterintelligence and Security Studies. September 2004. http://ctstudies.com/Document/Intelligence_Terrorism_Kalugin_oped_Sept_2004.html (accessed 17 February 2006).

Lyle, Peter A. “ Racial Profiling and the Fourth Amendment: Applying the Minority Victim Perspective to Ensure Equal Protection Under the Law.” http://www.bc.edu/bc_org/avp/law/lwsch/journals/bctwj/21_2/02_TXT.htm (accessed 27 March 2006).

MacDonald, Heather. “What We Don’t Know Can Hurt Us.” *City Journal*, 20 April 2004. http://www.city-journal.org/html/14_2_what_we_dont_know.html (accessed 17 Feb 2006) and http://www.frontpagemag.com/Articles/Printable.asp?ID=13053 (accessed 17 February 2006).

McCormick, Evan. “Jihad In America [*sic*].” *FrontPageMagazine.com*, 5 September 2003. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=9706 (accessed 17 February 2006).

Meir-Levi, David. “Connecting the South American Terror Dots.” *FrontPageMagazine.com*, 11 March 2004. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=14557 (accessed 17 February 2006).

Meyer, Josh. “Extremists Are Homing in on the Internet, Says Gonzales.” *Los Angeles Times* (17 August 2006): A17 [electronic document].

MSNBC. “Inspector: Homeland Security Database Flawed.” *MSNBC News Services* (12 July 2006). http://www.msnbc.msn.com/id/13822662/ (accessed 7 November 2006).

Philpott, Don. “The London Bombings: New Evidence Points to Al-Qaida and a New Terror Campaign.” *Homeland Defense Journal Special Report*, [2005]. http://www.homelanddefensejournal.com/pdfs/LondonBombing_SpecialReport.pdf (accessed 5 November 2006).

Pipes, Daniel. “A Call For Intelligent Profiling [by Frederick Schauer].” *New York Sun*, 30 December 2003. http://www.danielpipes.org/article/1385 (accessed 17 February 2006).

Pipes, Daniel. “[the Need to Name and] Know Thy Terrorists.” *New York Post*, 19 November 2002. http://www.danielpipes.org/article/943 (accessed 17 February 2006).

Pipes, Daniel. “[Maher Hawash:] The Terrorist Next Door.” *New York Post*, 12 August 2003. http://www.danielpipes.org/article/1195 (accessed 17 February 2006).

Pipes, Daniel. “PBS, Recruiting for Islam.” *New York Post*, 17 December 2002. http://www.danielpipes.org/article/982 (accessed 17 February 2006).

Pipes, Daniel. “Stealth Islamist: Khaled Abou El Fadl.” *Middle East Quarterly* (Spring 2004). http://www.danielpipes.org/article/1841 (accessed 17 February 2006).

Pipes, Daniel. “The Enemy Within.” *New York Post*, 24 January 2003. http://www.danielpipes.org/article/1009 (accessed 17 February 2006).

Pipes, Daniel. “Think Like a Muslim[, Urges “Across the Centuries”].” *New York Post*, 11 February 2002. http://www.danielpipes.org/article/118 (accessed 17 February 2006).

Robinson, Linda. “Plan of Attack.” *U.S. News & World Report*,1 August 2005. http://www.usnews.com/usnews/news/articles/050801/1terror.htm (accessed 12 November 2006).

Sageman, Marc. *E-Notes: Understanding Terror Networks*. Philadelphia, PA: Foreign Policy Research Institute, 2004. http://www.fpri.org/enotes/20041101.middleeast.sageman.understandingterrornetworks.html (accessed 31 May 2006).

Schwartz, Stephen. "The Holy War Foundation." *FrontPageMagazine.com*, 30July 2004. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=14435 (accessed 17 February 2006).

Shahar, Yael. "London Underground Partially Shut Down after Minor Explosions." The Institute for Counter-Terrorism, 21 July 2005. http://www.ict.org.il/spotlight/det.cfm?id=1094 (accessed 5 November 2006).

Spencer, Robert. "American Jihad." *FrontPageMagazine.com*, 11 March 2004. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=12524 (accessed 17 February 2006).

Spencer, Robert. "The Enemy is Not Just Al-Qaeda." *FrontPageMagazine.com*, 20 May 2004. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=13454 (accessed 17 February 2006).

Spencer, Robert. "The New Face of Al-Qaeda." *FrontPageMagazine.com*, 1 June 2004. http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=13591 (accessed 17 February 2006).

"Vulnerabilities in the Terrorist Attack Cycle." *STRATFOR* (Strategic Forecasting, Inc.), 29 September 2005. http://www.stratfor.com/products/premium/print.php?storyId=256319 (accessed 6 March 2006).

Whitlock, Craig. "Briton Used Internet As His Bully Pulpit." *The Washington Post, Monday, 8 August 2005*. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/07/AR2005080700890.html (accessed 17 February 2006).

Zawahiri, Ayman al-. Electronic mail to Muhammad Atef [translated], 15 April 1999. In Cullison, Alan. "Inside Al-Qaeda's Hard Drive." *The Atlantic Monthly* (September 2004). http://www.theatlantic.com/doc/200409/cullison (accessed 3 November 2006).

Zawahiri, Ayman al-. Letter to Abu Musab al-Zarqawi [translated], 9 Jul 2005. http://www.weeklystandard.com/Content/Public/Articles/000/000/006/203gpuul.asp (accessed 31 May 2006).

Unpublished Sources

Anonymous. "Understanding Islamist Militant Terrorism and Prevention Strategies." First Technologies, LLC., Federal Law Enforcement Training Center, Glynco, GA. Training Seminar, 16-17 September 2004 and 30 November 2004.

Boitnott, William, Federal Aviation Administration. Electronic correspondence, 6 September 2005.

Chechen Jihadi Documentation Video. http://www.ogrish.com/archives/footage_of_car_bomb_blowing_up_near_army_convoy_chechnya_2001_Sep_12_2004.html (accessed 5 November 2006).

Grynckewich, Alexus Major, USAF. Naval Postgraduate School, Monterey, CA. Group Discussion on Terrorist Financing, 5 June 2006.

Jihadi recruitment video. Presented in "Understanding Islamist Militant Terrorism and Prevention Strategies." First Technologies, LLC., Federal Law Enforcement Training Center, Glynco, GA. Training Seminar, 16-17 September 2004.

Mannes, Ariel Benjamin, Special Agent, Transportation Security Administration, Department of Homeland Security. "Interagency Intelligence Sharing and Analysis: Resources in the Homeland Security Reporting Process." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 20 October 2005.

McCreary, John F., Defense Intelligence Agency. Presentation on Indications and Warning Analysis. Lecture with handouts. Naval Postgraduate School, Monterey, CA. Lecture, 22 February, 2006.

Nasr, Seyyed Vali Reza. Series of lectures on Islamic Fundamentalism at the Naval Postgraduate School, Monterey, CA, 25 September-23 October 2006.

Odisho, Joseph, U.S. Government contract linguist. Personal conversation during USAF Special Investigations Academy Critical Threat Counterintelligence Collections Course, 2005.

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). "Terrorism & Attacks on the Civil Aviation Industry." International Counter-Terrorism Officers [*sic*] Association 2nd Annual Conference, Las Vegas, NV. Lecture, 29 September 2004.

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). "Understanding Terrorist Ideology." International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). “Issues in Transportation Related [*sic*] Terrorism.” International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 20 October 2005.
Rowland, John C. “The New Terrorism: Global Jihad.” International Counter-Terrorism Officers [*sic*] Association 2nd Annual Conference, Las Vegas, NV. Lecture, 28 September 2004.

Suspected terrorist pre-operational reconnaissance video, seized by Canadian authorities. Presented by Rocke, Steve, Constable, Peel Regional Police (Ontario, Canada). “Understanding Terrorist Ideology.” International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

Sutton, Rory. US Army Corps of Engineers, Jacksonville, FL. Interview, 15 December 2004. Followed by correspondence, 25 August 2005.

Teft, Bruce. “Terrorism Awareness—Islamic Terrorism: Origins and Prevention.” International Counter-Terrorism Officers [*sic*] Association 3rd Annual Conference, Orlando, FL. Lecture, 18 October 2005.

U.S. Government Counterterrorist Training Group Special Seminar on Surveillance Detection, September-October 1997.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Headquarters, Air Force Office of Special Investigations
   Andrews AFB, Maryland